SIMMONS HANLY CONROY, LLC
Jason 'Jay' Barnes (admitted *pro hac vice*)
An Truong (admitted *pro hac vice*)
Eric Johnson (admitted *pro hac vice*)
112 Madison Avenue, 7th Floor
New York, NY 10016
Telephone: (212) 784-6400
Facsimile: (212) 213-5949
jaybarnes@simmonsfirm.com
atruong@simmonsfirm.com
ejohnson@simmonsfirm.com

KIESEL LAW LLP
Jeffrey A. Koncius, State Bar No. 189803
Nicole Ramirez, State Bar No. 279017
8648 Wilshire Boulevard
Beverly Hills, CA 90211-2910
Telephone: (310) 854-4444
Facsimile: (310) 854-0812
koncius@kiesel.law

SCOTT+SCOTT ATTORNEYS AT LAW LLP
Joseph P. Guglielmo (admitted pro hac vice)
Ethan Binder (admitted pro hac vice)
230 Park Ave., 17th Floor
New York, NY 10169
Telephone: (212) 223-6444
Facsimile: (212) 223-6334
jguglielmo@scott-scott.com
ebinder@scott-scott.com

LOWEY DANNENBERG, P.C.
Christian Levis (admitted *pro hac vice*)
Amanda Fiorilla (admitted pro hac vice)
44 South Broadway, Suite 1100
White Plains, NY 10601
Telephone: (914) 997-0500
Facsimile: (914) 997-0035
clevis@lowey.com
afiorilla@lowey.com

LIEFF CABRASER HEIMANN & BERNSTEIN, LLP
Michael W. Sobol, State Bar. No. 194857
Melissa Gardner, State Bar No. 289096
275 Battery Street, 29th Floor
San Francisco, CA 94111-3339
Telephone: (415) 956-1000
Facsimile: (415) 956-1008
msobol@lchb.com
mgardner@lchb.com

LIEFF CABRASER HEIMANN & BERNSTEIN, LLP
Douglas Cuthbertson (admitted *pro hac vice*)
250 Hudson Street, 8th Floor
New York, NY 10013
Telephone: 212 355-9500
Facsimile: 212-355-9592
dcuthbertson@lchb.com

Attorneys for Plaintiffs and the Proposed Class
**Additional counsel listed on signature page*

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO DIVISION

JOHN DOE I, et al. on behalf of themselves and all others similarly situated,

Plaintiffs,

v.

GOOGLE LLC,

Defendant.

This document applies to: All Actions

Case No. 3:23-cv-02431-VC
Consolidated with: 3:23-cv-02343-VC

CLASS ACTION

****FILED UNDER SEAL****

SECOND AMENDED CONSOLIDATED CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

Judge: Hon. Vince Chhabria
Action Filed: May 12, 2023
Trial Date: Not Set

TABLE OF CONTENTS

TABLE OF CONTENTS
(continued)

Page

I. INTRODUCTION

1. Plaintiffs challenge Google's use of website tracking technology to intentionally obtain their "Health Information" as defined by the Federal Trade Commission and protected under the Health Information Portability and Accountability Act ("HIPAA").

2. While promising that Google would collect Health Information only if individuals "choose to provide it," Google collected the contents of Plaintiffs' communications about their doctors, treatments, conditions, bill payments, prescription drugs, patient portal activities, appointment requests, and other information relating to their health and healthcare through Google-designed communications tracking technologies on Health Care Provider web-properties (websites and apps). Plaintiffs did not know of Google's conduct, could not have known, and did not consent. Google engaged in the same conduct as to all members of the Class.

3. Although Google's acquisition of Plaintiffs' Health Information is an actionable wrong on its own, Google compounds the intrusion by using it for numerous purposes that Plaintiffs do not reasonably expect in contravention of direct promises by Google. These include using Health Information to build health-related user profiles by assigning Plaintiffs and their communications to categories or "segments"; to develop, improve, inform, and profit from the data via myriad Google advertising products; to target users for Google's business purposes even when (and if ever) it is not targeting them with ads; to improve Google's search algorithms, machine learning and artificial intelligence models, including models used in advertising; and in connection with other wholly unrelated business pursuits.

4. At all relevant times, Google acted with intent. Recently unsealed documents show that, no later than 2017, Google targeted the healthcare industry for expanding Google Analytics. Google knew that Health Care Providers could not use Google's third-party tracking technologies as advertised, to track Health Care Providers' "customers," who are patients, without disclosing Health Information to Google, and yet, Google targeted them anyway. Google also knew that its marketing materials and adhesion form contracts with Health Care Providers suggested they *could* use Google's technologies without transmitting Health Information to Google. Yet Google did not

issue any warning to Health Care Providers that its tracking technology was collecting their patients' Health Information until March 2023—years after the source code proliferated across and within an estimated 91% of Health Care Provider web properties, and even then, Google only did so after federal regulators and journalists highlighted the problem. Instead, for at least seven years, Google stayed quiet, until it could not do so any longer, because it benefited from obtaining Plaintiffs' and Class members' Health Information. Google's willful actions violated the medical privacy rights of millions.

5. Plaintiffs bring this action on behalf of themselves and all others similarly situated to hold Google accountable for its actions.

II. PARTIES

6. Plaintiff John Doe I is a resident of Wisconsin.

7. Plaintiff John Doe II is a resident of California.

8. Plaintiff John Doe IV is a resident of California.

9. Plaintiff John Doe V is a resident of Florida.

10. Plaintiff Jane Doe I is a resident of Maryland.

11. Plaintiff Jane Doe VI is a resident of Texas.

12. Plaintiff Jane Doe VII is a resident of Illinois.

13. Defendant Google LLC is a Delaware Limited Liability Company headquartered at 1600 Amphitheatre Parkway, Mountain View, California ("Defendant" or "Google"), whose membership interests are entirely held by its parent holding company, Alphabet, Inc. ("Alphabet"), headquartered at the same address. All operations relevant to this Complaint are run by Google.

III. JURISDICTION, VENUE, AND ASSIGNMENT

14. This Court has personal jurisdiction over Google because it is headquartered in this District and Google consents to this Court's jurisdiction in its current and prior Google Terms of Service. Further, Google designed, contrived and effectuated the collection of Plaintiffs' and Class

Members' Health Information from the State of California, and Google maintains and/or oversees systems designed to effectuate this collection within the State of California.

15. Venue is proper in this District because Google is headquartered here and because Google's current and prior Terms of Service purport to bind Plaintiffs and Class Members to bring disputes in this District.

16. Assignment of this case to the San Jose Division was proper pursuant to Civil Local Rule 3-2(e) because a substantial part of the events or omissions giving rise to Plaintiffs' claims occurred in Santa Clara County, California. These consolidated actions have properly been reassigned to the San Francisco Division pursuant to Civil Local Rule 3-12(f).

17. This Court has subject matter jurisdiction over the federal claims in this action.

18. This Court has subject matter jurisdiction over this entire action pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d), because this is a class action in which the amount in controversy exceeds $5,000,000, and at least one member of the class is a citizen of a state other than the state in which Google maintains its headquarters (California) and in which it is incorporated (Delaware).

19. This Court has supplemental jurisdiction over the state law claims in this action pursuant to 28 U.S.C. § 1367, because the state law claims form part of the same case or controversy as those that give rise to the federal claims.

20. This Court has equitable jurisdiction to entertain claims and award remedies that are equitable in nature because Plaintiffs lack an adequate remedy at law. Monetary damages cannot make Plaintiffs whole for the totality of the harm to privacy rights, rights to dignity, rights to self-determination and rights to control access and use of their Health Information, or for the harm to societal and personal expectations of privacy and justice violated by Google's conduct alleged herein. Monetary damages cannot make Plaintiffs whole for the harms caused by Google's alleged violations of statutes which do not provide for private rights of action, or for Google's alleged violations of laws which limit their application to particular aspects of the broad-ranging pattern of activity by Google alleged herein. Further, there is no adequate remedy at law and an

award of damages under the law will not necessarily encompass profits or benefits Google unjustly earned as a result of its unauthorized post-collection use of Plaintiffs' and Class Members' Health Information, which it may not retain under California law. Additionally, Plaintiffs may be unable to obtain full relief on a class-wide basis under each legal claim and/or on behalf of a certified Class due to different requirements of proof (e.g., mens rea and reliance) and the Court may permit Plaintiffs to plead both damages and, in the alternative, equitable remedies at the early pleadings stage. In addition, the Court has equitable jurisdiction to issue injunctions that serve different purposes and remedy different harms than retrospective monetary damages.

IV. DEFINITIONS

21. As used in this Complaint,

a. "Health Information" means "anything that conveys information that enables an inference about a consumer's health and anything that conveys information – or enables an inference – about a consumer's health"[1] and includes any identifiable information that relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual.

b. "Health Care Provider" means a person that is a "covered entity" under HIPAA or the California Medical Information Act.

c. "Google Source Code" means and includes the code and all components of Google's third-party tracking technologies discussed herein.

[1] *See* Elisa Jillson, *Protecting the Privacy of Health Information: A Baker's Dozen Takeaways from FTC Cases*, FED. TRADE COMM'N BUSINESS BLOG, https://www.ftc.gov/business-guidance/blog/2023/07/protecting-privacy-health-information-bakers-dozen-takeaways-ftc-cases; 45 C.F.R. § 160.103 (unless otherwise stated, all hyperlinks cited herein were last visited on or around August 10, 2024). Plaintiffs also append certain documents cited herein that are difficult to access online, or for which there is a reasonable chance the documents will cease to be available online either entirely, or in their current form after this pleading is filed, as Exhibits, identified in the Appendix to this Complaint.

V. FACTUAL ALLEGATIONS

A. Google's Business

22. Google's parent company, Alphabet, divides its business into three segments: Google Services, Google Cloud, and "other Bets," which include Google's other business pursuits. Google Services include Google's interconnected analytics, advertising and measurement platforms, and generates revenues primarily through advertising.[2]

B. Google's Third-Party Tracking Technologies

23. Google has been the market leader in online advertising for well over a decade and, in furtherance of that, has built and acquired a slew of internet tracking technology systems that enable it to identify and provide online access to "audience[s]" of individuals expected to respond favorably and/or profitably to advertisements and other messages that Google delivers across "owned and operated" platforms, including Google Search, YouTube, Maps, as well as other third-party websites within its ad network. The same technology also allows Google to monitor and collect data from the user's response to these ads.

24. To enable this tracking, Google deposits small text files called "cookies" on the computers or mobile devices of individuals who visit websites where Google source code is present. Both classic third-party cookies, and third-party cookies disguised as first party cookies (to circumvent cookie blockers, as discussed further below), are placed by Google and transmitted to Google with other information Google's tracking technologies intercept about the individual and their interactions with the site in real-time back to specific Google-owned domains ("endpoints").

25. **Google Ads** is present on Plaintiffs' Health Care Provider web properties. It is the overarching platform through which Google sells, delivers, tracks, and learns from advertising on Google's networks, including through Search Ads, Display Ads, Performance Max Ads, Smart Ads, and others. Source code for Google Ads products transmit data to the following non-

[2] ALPHABET, INC., Annual Report (Form 10-K) (Dec. 31, 2022), https://abc.xyz/investor/static/pdf/20230203_alphabet_10K.pdf.

exhaustive list of advertising endpoints: www.google.com/pagead/1p-user-list; www.google.com/maps; www.google.com/ads/ga-audiences; adservice.google.com; www.google.com/ads/measurement; fcmatch.google.com; ade.googlesyndication.com; pagead2.googlesyndication.com; tpc.googlesyndication.com; www.googleadservices.com (referred to below as "Ads Code"); as well as: www.doubleclick.net; securepubads.g.doubleclick.net; bid.g.doubleclick.net; googleads.g.doubleclick.net; stats.g.doubleclick.net; and cm.g.doubleclick (referred to below as "Doubleclick Ads Code") "Ads Code," and "Doubleclick Ads Code," collectively are referred to below as "Ads Source Code."

26. **Google Analytics** is present on Plaintiffs' Health Care Provider web properties. It is a platform designed to work in concert with Google Ads, through which Google obtains additional detailed information about users and their activity on websites Google does not, itself, own and operate. Google Analytics source code transmits information to the endpoints www.google-analytics.com and/or analytics.google.com ("Analytics Code" or "Analytics Source Code").

27. Google's Ads and Analytics products are designed to work together and share data across systems. To facilitate this, Google maintains the information collected by all of the products on Healthcare Provider properties discussed herein in such a way that it can used in another system at any time.[3] Google encourages its customers (including Plaintiffs' Healthcare Providers) to join data from multiple systems, to "import your Analytics conversions and audiences into your Google Ads account;" to "analyze your Display & Video 360 data in Analytics" to "analyze your Search Ads 360 data in Analytics," and to "[a]pply your Analytics insights to Google Ad Manager to optimize the user experience on your sites and apps, and improve monetization."[4] "The Google

[3] *Analytics*, GOOGLE MARKETING PLATFORM, https://marketingplatform.google.com/about/analytics/ (under the sub-heading *Designed to work together*, Google explains that advertisers should "use Analytics with other Google solutions to get a complete understanding of [their] marketing efforts and enhance performance").

[4] *Analytics 360*, GOOGLE MARKETING PLATFORM, https://marketingplatform.google.com/about/analytics-360/features/#integrations.

Ads integration is available to all Analytics accounts," and when integration occurs, "[a]ll default Analytics data" is used like any other data obtained by Google's advertising products.[5]

28. **Google Tag** source code, consistent with Google's integrated approach to advertising and analytics, can be configured to transmit information to any Google endpoint. "The Google tag lets you send data from your website to connected Google product destinations to help you measure the effectiveness of your website and ads. After you place the Google tag on your website, it sends to linked Google product destinations, such as Google Ads and Google Analytics. You can use a single Google tag implementation for all your products and accounts."[6] It is javascript code that appears as "gtag" in web traffic, or the presence of which can be deduced from the contemporaneous transmission of an event to both Google Ads and Google Analytics endpoints. Google expressly recommends that the "tag should be installed on every page of your website."[7]

29. **Google Tag Manager ("GTM")** is a tag management system that "has the same functionality as the Google tag" except that it consolidates "tags" not only from Google, but also from other advertising and analytics providers that surveil users' activities across the Internet.[8] GTM streamlines the process of setting up and using both Google's and other entities' "tags" reducing the technical complexity of establishing surveillance by multiple entities receiving multiple streams of data from a particular website, as well as eliminating or reducing delays inherent in loading tracking code from multiple sources. GTM provides "native" sharing for 79 advertising and analytics providers and at least 879 others in its "templates" section.[9] Whether a

[5] *About Remarketing Audiences in Analytics*, GOOGLE ANALYTICS HELP, https://support.google.com/analytics/answer/2611268.

[6] *Configure your Google tag settings*, GOOGLE ADS HELP, https://support.google.com/google-ads/answer/12131703.

[7] *Use the Google Tag for Google Ads Conversion Tracking*, GOOGLE ADS HELP, https://support.google.com/google-ads/answer/7548399.

[8] *About Google Tag Manager*, TAG PLATFORM, https://developers.google.com/tag-platform/tag-manager.

[9] *See Supported Tags*, GOOGLE TAG MANAGER HELP, https://support.google.com/tagmanager/answer/6106924? (listing "native") and https://tagmanager.google.com/gallery/#/?page=1 (others)

particular website uses GTM can be determined from transmissions to the endpoint googletagmanager.com, or from the "gtm" value, set to an alphanumeric value that corresponds to the associated GTM account in network traffic.

30. Collectively, Plaintiffs refer to the above-described technologies as "Google Source Code" herein.

31. Google maintains sole control over the code for the tracking technologies described above and makes them available to Health Care Providers in a standard copy-and-paste format.

32. The "Google Source Code" at issue here is designed and works substantially the same for all web-properties i.e. there is no "health industry specific" version of the products.

C. Google's Acquisition of the Plaintiffs' Health Information

33. Plaintiffs are patients of United States Health Care Providers who routinely visit their Health Care Providers' web properties for purposes relating to their mental or physical health, conditions, care, and billing, and who made such visits within one year of the date this action was filed. Plaintiffs' Health Care Providers, in turn, are among several thousand HIPAA- and CMIA-covered entities where Google is collecting Health Information through its source code on Health Care Provider web-properties. When Plaintiffs visited and used their Health Care Providers' web properties, Google obtained their Health Information.

1. Google Source Code is Extensively Integrated in Plaintiffs' Health Care Provider Websites

34. To provide the Court with visual examples from their forensic investigations which support Plaintiffs' allegation that Google obtained their Health Information, Plaintiffs have attached a series of screenshots in Exhibit 1 that are extracted from data recordings showing specific Health Information communications, their content, and identifiers Google was intercepting from Plaintiffs' Health Care Providers' websites at or around the time this action commenced in May 2023. Plaintiffs also submit excerpts of the results of a broader analysis of Request Headers on Plaintiffs' Health Care Provider web properties (and thousands of others), showing transmissions by Google Ads and Analytics from their Health Care Providers to Google,

as Exhibit 2. Because Plaintiffs' actual visits to their Health Care Providers' websites were for healthcare purposes and not in anticipation of litigation, counsel did not create records of Google's interceptions during those visits. Nevertheless, and below, Plaintiffs submit an accounting of Plaintiffs' communications and activities on their Health Care Provider web properties, and evidence their counsel gathered shortly thereafter regarding transmissions via Google's third-party tracking technologies on and throughout those web properties.[10]

a. Gunderson – John Doe I

35. Plaintiff John Doe I is a patient of Gundersen Health System ("Gundersen").

36. Plaintiff John Doe I visits the Gundersen web property at www.gundersenhealth.org when he needs to interact with his Health Care Provider, including to schedule appointments, identify a specialist for his medical needs, review test results, communicate with his providers, and review or pay his medical bills. Among other visits in the past several years, Plaintiff visited the web property regularly, including on or around [redacted]

37. Plaintiff generally commenced each visit by visiting the homepage. Hyperlinks on the Gundersen web property homepage include: "Find a Provider," "Care & Treatment," "Patients and Visitors," "Health and Wellness," "Your care options," "Find care near you," "Pay my Bill," "Log in to MyChart," as well as a hyperlink entitled "MyChart," which also takes the visitor to the MyChart login page. Gundersen's patient portal is powered by Epic.

38. Among other actions, from the homepage, Plaintiff clicked on the link to sign in to his "MyChart" patient portal and searched for medical professionals specific to his medical needs, including searches for a [redacted], and also communicated with Gundersen about payment of bills; about scheduling appointments; about viewing his medical records, medications, and lab results within the patient portal; about his doctors, including [redacted].

[10] Information useful for interpreting the contents of Exhibits 1 and 2 is provided in Sections V(C)(2)-(3), *infra*.

[redacted], and about his specific conditions or treatments, including [redacted]. Google intercepted all of these communications, including those made beyond the home page regarding his specific doctors, conditions, and treatments.

39. Review via developer tools showed that, at or around the time this action was filed, Ads Code, Doubleclick Ads Code, and Analytics Code all were extensively integrated on the Gundersen web property, including on the home landing page and numerous other pages concerning, containing, and reflecting Health Information and related communications, which Google intercepted concerning every visitor to the web property, including Plaintiff.

40. Ads Code was present at the URLs :

https://www.gundersenhealth.org/services/pregnancy-birth/before-baby-preparing-for-pregnancy;
https://www.gundersenhealth.org/services/urology;
https://www.gundersenhealth.org/find-a-doctor;
https://www.gundersenhealth.org/services/mychart-e-visit;
https://www.gundersenhealth.org/patients-visitors/cash-pay-services; and
https://www.gundersenhealth.org/patients-visitors/scheduled-for-an-upcoming-procedure,

among many others. *See, e.g.*, Ex. 1, Gundersen Request # 722 (intercepting communication regarding search for Dr. Joseph M. Endrizzi, a specialist in urology); *see also* Ex. 2 at 1-3.

41. Doubleclick Ads Code was also present at the URLs above, among many others. *See id.*; *see, e.g.,* Ex. 1, Gundersen Request # 720 (intercepting communication regarding search for Dr. Joseph M. Endrizzi, a specialist in urology); *see also* Ex. 2.

42. Analytics Code was present at the URLs above, among many others. *See id.*; *see, e.g.,* Ex. 1, Gundersen Request # 568 (intercepting communication regarding search for Dr. Joseph M. Endrizzi), Gundersen Request # 694 (intercepting communication regarding booking an appointment with Dr. Joseph M. Endrizzi). It was also present at the URL https://www.gundersenhealth.org/patients-visitors/scheduled-for-an-upcoming-procedure, which is accessible from the home page by clicking on "Patients and Visitors," and then clicking a link

to "Learn More" "pre-visit information" for upcoming scheduled procedures. *See, e.g.,* Ex. 1, Gundersen Request # 830; *see also* Ex. 2 at 1-3.

b. Kaiser – John Doe II and John Doe IV

43. Plaintiffs John Doe II and John Doe IV are patients of Kaiser Permanente ("Kaiser"). Kaiser operates the web property https://healthy.kaiserpermanente.org/.

44. Both Plaintiffs John Doe II and John Doe IV visit the Kaiser web property at healthy.kaiserpermanente.org when they need to interact with their Health Care Provider, including to schedule appointments, identify a specialist for their respective medical needs, review test results, communicate with providers, and review or pay medical bills. Among other visits in the past several years, Plaintiff John Doe II visited the web property regularly, including on or around October 10, 2019, December 27, 2020, December 21, 2021, December 28, 2022, November 4, 2023, and April 25, 2024, and Plaintiff John Doe IV visited the web property multiple times during the class period, including on or around June 29, 2018, September 26, 2019, July 25, 2020, January 2, 2022, January 24, 2023, May 22, 2023, July 11, 2023, July 14, 2023, July 19, 2023, November 1, 2023, and December 8, 2023.

45. Both Plaintiffs generally commenced each visit by visiting the homepage. Hyperlinks on the Kaiser web property homepage include: "Shop Plans," "Doctors & Locations," "Health & Wellness," "Get Care," "Pay Bills," and "sign in." Among other actions, from the homepage, Plaintiff John Doe II clicked on the link to "sign in" to his patient portal and communicated with Kaiser by conducting doctor searches specific to his medical needs, including searches for a [redacted]; and also communicated with Kaiser about payment of bills; about scheduling appointments; about viewing his medical records, medications, and lab results within the patient portal; about his doctors, including [redacted]; and about his specific conditions or treatments, including b[redacted].

46. Among other actions, from the homepage, Plaintiff John Doe IV clicked on the link to "sign in" to his patient portal and communicated with Kaiser by conducting doctor searches

specific to his medical needs, including searches for a primary care provider; and also communicated with Kaiser about scheduling appointments; viewing his medical records, test results, and visit summaries within the patient portal; about his doctors, including Dr. William [redacted]; and about his specific conditions or treatments, including [redacted].

47. Review via developer tools showed that, at or around the time this action was filed, Ads Code, Doubleclick Ads Code, and Analytics Code all were extensively integrated on the Kaiser web property, including on the home landing page and numerous other pages concerning, containing, and reflecting Health Information and related communications, which Google intercepted concerning every visitor to the web property, including Plaintiffs.

48. Ads Code was present at the URLs :

https://healthy.kaiserpermanente.org/northern-california/consumer-sign-on#/signon
https://healthy.kaiserpermanente.org/billpay
https://healthy.kaiserpermanente.org/health-wellness/health-encyclopedia/he.cancer-pain.tv7310#acl2396
https://healthy.kaiserpermanente.org/health-wellness/health-encyclopedia/he.obsessive-compulsive-disorder-ocd.hw169097

among many others. *See, e.g.* Ex. 1, Kaiser Request # 417 (intercepting communication that user reviewed an article about Type 2 Diabetes titled "*What is Type 2 Diabetes?"*), Kaiser Request # 875 (intercepting communication regarding access to bill pay page from patient portal access page), Kaiser Request # 611 (intercepting communication from inside patient portal showing that patient's doctor was Patrick Avanessian, a specialist in Family Medicine); *see also* Ex. 2 at 4-5.

49. Doubleclick Ads Code was present at the URLs above, among many others. *See, e.g.* Ex. 1, Kaiser Request # 405 (intercepting communication that patient was reviewing an article about Type 2 Diabetes), Kaiser Request # 867 (intercepting communication regarding access to bill pay from patient portal access page), Kaiser Request # 2223 (intercepting communication regarding interactions with insurance plan page for Medicare), Kaiser Request # 318 (intercepting communication that patient had logged-into the patient portal), Kaiser Request # 727 (intercepting

communication from inside patient portal showing that patient's doctor was Patrick Avanessian, a specialist in Family Medicine)*; see also* Ex. 2 at 4-5.

50. Analytics Code was present at the URLs above, among many others. *See, e.g.*, Ex. 1, Kaiser Request # 1649 (intercepting communication identifying patient's doctor as Vasantha Ravishankar), Kaiser Request # 1718 (same and with confirmation that patient had signed-in to My Doctor Online); *see also* Ex. 2 at 4-5.

51. On or around May 6, 2024, Kaiser posted a notification to its website announcing that "On October 25, 2023, Kaiser Permanente determined that certain online technologies (commonly known as cookies or pixels) installed on our websites and mobile applications may have transmitted personal information to our third-party vendors Google, Microsoft Bing, and X (Twitter) when members and patients accessed our websites or mobile applications."[11] The notice states that Kaiser "conducted a voluntary internal investigation into the use of these online technologies, and subsequently removed these online technologies from our websites and mobile applications. In addition, Kaiser Permanente has implemented additional measures with the guidance of experts to safeguard against recurrence of this type of incident."[12] Reports indicate that Kaiser sent notice of this disclosure to approximately 13.4 million individuals, which suggests that Kaiser believes that every one of its approximately 12.5 million members' Health Information was compromised, as well as the Health Information of others to whom Kaiser owes a duty of confidentiality.[13]

c. <u>Tallahassee Memorial HealthCare – John Doe V</u>

52. Plaintiff John Doe V is a patient of Tallahassee Memorial HealthCare ("TMH").

53. Plaintiff John Doe V visits the TMH web property at www.tmh.org when he needs to interact with his Health Care Provider, including to schedule appointments, identify a specialist

[11] Ex. 3, *Important notice about a privacy matter*, KAISER PERMANENTE (May 6, 2024), https://healthy.kaiserpermanente.org/washington/alerts/p3/privacy-matter.

[12] *Id.*

[13] David Bloxberg, *Latest Kaiser Data Breach Affects 13.4 Million Patients*, VIPRE (Apr. 29, 2024), https://vipre.com/blog/latest-kaiser-data-breach-affects-134-million-patients/.

for his medical needs, review test results, communicate with his providers, and review or pay his medical bills. Among other visits in the past several years, Plaintiff visited the web property on or around [redacted].

54. Plaintiff generally commenced each visit by visiting the homepage. Hyperlinks on the TMH web property homepage include: "Find a Doctor," "Pay My Bill," "Services," and "Patient Portal" or "Patient Portals" (the text has been modified since 2022). TMH's patient portal is powered by Cerner.[14] The homepage also contains a magnifying glass icon, which opens a search bar containing "Quick Links," including one for "Health & Wellness," and allows users to "Search the site." Among other actions, from the homepage, Plaintiff clicked on the link to access his patient portal and searched for medical professionals specific to his medical needs, including searches for a [redacted], and also communicated with TMH about payment of bills; about scheduling appointments; about viewing his medical records, medications, and lab results within the patient portal; about his doctors, including [redacted], and about his specific conditions or treatments, including [redacted].

55. Review via developer tools showed that, at or around the time this action was filed, Doubleclick Ads Code and Analytics Code were extensively integrated on the TMH web property, including on the home landing page and numerous other pages concerning, containing, and reflecting Health Information and related communications, which Google intercepted concerning every visitor to the web property, including Plaintiff.

56. Doubleclick Ads Code was present on the TMH home page. *See, e.g.,* Ex. 2 at 12.

57. Analytics Code was present on the home page and at the URLs https://www.tmh.org/services/orthopedics/hip-replacement-surgery, and https://www.tmh.org/healthcare-professionals/lab-services; among many others. *See, e.g. id.*

[14] *See* https://www.tmh.org/patients-and-visitors/patient-portals-at-tmh/mytmh-patient-portal.

d. MedStar – Jane Doe I

58. Plaintiff Jane Doe I is a patient of MedStar Health ("MedStar").

59. Plaintiff Jane Doe I visits the MedStar web property at www.medstarhealth.org. when she needs to interact with her Health Care Provider, including to schedule appointments, identify a specialist for her medical needs, review test results, communicate with her providers, and review or pay her medical bills. Among other visits in the past several years, Plaintiff visited the web property regularly, including in 2022 and 2023, and on or around [redacted].

60. Plaintiff generally commenced each visit by visiting the homepage. Hyperlinks on the MedStar web property homepage include: "Healthcare Services," "Find a Doctor," and "Patient Portal." MedStar's patient portal is powered by Cerner. There are also links to access information about specific services including "Gastroenterology," "Orthopedics," and "Cancer." Additional hyperlinks include one to a "FAQ Page" to "Get answers to billing and insurance questions." The homepage also contains a search bar inviting visitors to search for "Providers, Services and More." Among other actions, from the homepage, Plaintiff clicked on the link to access her patient portal and searched for medical professionals specific to her medical needs, including searches for a [redacted] and also communicated with MedStar about payment of bills; about scheduling appointments; about viewing her medical records, medications, and lab results within the patient portal, and about her specific conditions or treatments, including [redacted].

61. Review via developer tools showed that, at or around the time this action was filed, Ads Code, Doubleclick Ads Code, and Analytics Code all were extensively integrated on the MedStar web property, including on the home landing page and numerous other pages concerning, containing, and reflecting Health Information and related communications, which Google intercepted concerning every visitor to the web property, including Plaintiff.

62. Ads Code was present at the URLs :

https://www.medstarhealth.org/doctors/emily-c-keadle-fnp-dnp;
https://www.medstarhealth.org/locations/gastroenterology-at-medstar-washington-hospital-center;
https://www.medstarhealth.org/services/gastrointestinal-cancers; and

https://www.medstarhealth.org/mymedstar-patient-portal/billing,

among many others. *See, e.g.,* Ex. 1, MedStar Request # 1504 (intercepting communication regarding search for Dr. Vandha Sharma), MedStar Request # 1236 (intercepting communication regarding access to MyMedStar Patient Portal); *see also* Ex. 2 at 6-7.

63. Doubleclick Ads Code was present at the URLs above, among many others. *See, e.g.,* Ex. 1, MedStar Request # 720 (intercepting communication regarding patient's search for Dr. Joseph M. Endrizzi, a specialist in urology), MedStar Request # 1493 (intercepting communication regarding search for Dr. Vandha Sharma), MedStar Request # 1596 (intercepting communication regarding access to MyMedStar Patient Portal); *see also* Ex. 2 at 6-7.

64. Analytics Code was present at the URLs above, among many others. *See, e.g.,* Ex. 1, MedStar Request # 1239 (intercepting communication regarding access to MyMedstar Patient Portal), MedStar Request # 1443 (intercepting communication regarding patient's search for a doctor with a specialty in diabetes within a 25-mile radius of zip code 25000), MedStar Request # 1523 (intercepting communication regarding services of Dr. Vandha Sharma, an Endocrinologist); *see also* Ex. 2 at 6-7.

e. Shannon Medical – Jane Doe VI

65. Plaintiff Jane Doe VI is a patient of Shannon Medical Center ("Shannon Medical").

66. Plaintiff Jane Doe VI visits the Shannon Medical web property at www.shannonhealth.com when she needs to interact with her Health Care Provider, including to schedule appointments, identify a specialist for her medical needs, review test results, communicate with her providers, and review or pay her medical bills. Among other visits in the past several years, Plaintiff visited the web property on or around [redacted]

[redacted]

67. Plaintiff generally commenced each visit by visiting the homepage. Hyperlinks on the Shannon Medical web property homepage include: "Wait Times," "Providers," Services," "Find A Service," and "MyChart," which takes visitors to a MyChart login page where they are prompted to "Register For MyChart" and "Sign Into MyChart" amongst other options. Shannon Medical's patient portal is powered by Epic. From the homepage, Patients can click a link to "reserve a spot in line" at "Urgent Care." There are also links to access information about specific services including "Cancer Care," "OB/GYN," and "Orthopedics." The homepage also contains a search bar. Among other actions, from the homepage, Plaintiff clicked on the link to access her patient portal and searched for medical professionals specific to her medical needs, including searches for a [redacted], and also communicated with Shannon Medical about payment of bills; about scheduling appointments; about viewing her medical records, medications, and lab results within the patient portal, about her healthcare providers, including [redacted], and about her specific conditions or treatments, including [redacted]

68. Review via developer tools showed that, at or around the time this action was filed, Doubleclick Ads Code and Analytics Code were integrated on the Shannon Medical web property, including on the home landing page, which concerns, contains, and reflects Health Information and related communications

69. Doubleclick Ads Code was present at the URL https://www.shannonhealth.com/. *See, e.g.,* Ex. 2 at 8.

70. Analytics Code was also present at the above URL, as well as https://www.shannonhealth.com/patients-visitors/billing-and-insurance/no-surprises-act-notice/, which contains hyperlinks including one to "Pay my Bill." *See, e.g., id.*

f. Edward-Elmhurst Health – Jane Doe VII

71. Plaintiff Jane Doe VII is a patient of Edward-Elmhurst Health.

72. Edward-Elmhurst's patient portal is powered by Epic.

73. Plaintiff Jane Doe VII visits the Edward-Elmhurst web property at www.eehealth.org when she needs to interact with her Health Care Provider, including to schedule appointments, identify a specialist for her medical needs, review test results, communicate with her providers, and review or pay her medical bills. Among other visits in the past several years, Plaintiff visited the web property on or around [redacted].

74. Plaintiff generally commenced each visit by visiting the homepage. Hyperlinks on the Edward-Elmhurst web property homepage include: "MyChart Login," "Find Care Now," "Schedule Online," "Find a Doctor," and "Search our Services." Under the heading "I am a patient," the homepage presents additional hyperlinks for "Patient portal/MyChart," and "Pay my bill," "Wait Times," "Providers," Services," "Find A Service," and "MyChart," which takes visitors to a MyChart login page where they are prompted to "Register For MyChart" and "Sign Into MyChart" amongst other options. Patients can click a link to "reserve a spot in line" at "Urgent Care." There are also links to "gauge your health" and "Assess Your Risk" by completing a five-minute online assessment, in categories for Heart, Depression, Stroke, and Diabetes. The homepage also presents a search bar. Among other actions, from the homepage, Plaintiff clicked on the link to access her patient portal and searched for medical professionals specific to her medical needs, including searches for a [redacted], and also communicated with Edward-Elmhurst about payment of bills; about scheduling appointments; about viewing her medical records, medications, and lab results within

the patient portal, and about her healthcare providers, including [redacted].

75. Review via developer tools showed that, at or around the time this action was filed, Ads Code, Doubleclick Ads Code, and Analytics Code all were extensively integrated on the Edward-Elmhurst web property, including on the home landing page and numerous other pages concerning, containing, and reflecting Health Information and related communications, which Google intercepted concerning every visitor to the web property, including Plaintiff.

76. Ads Code was present at the URLs :

https://www.eehealth.org/services/behavioral-health/programs/eating-disorders/;
https://www.eehealth.org/find-a-doctor/search-results/;
https://www.eehealth.org/patients-visitors/manage-my-costs-and-billing/billing/financial-assistance/; and
https://www.eehealth.org/services/plastic-surgery/schedule-consultation-request/,

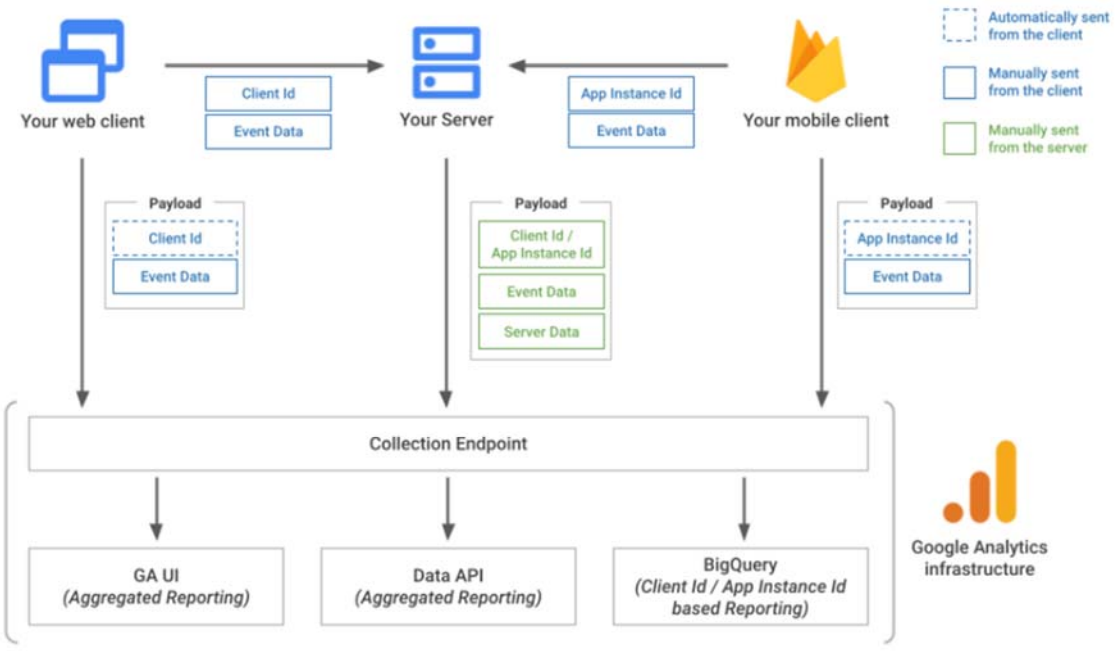
among many others. *See* Ex. 1, Edward-Elmhurst Request # 895 (intercepting communication regarding search for Dr. Julie C. Lopatka); *see also* Ex. 2 at 9-11.

77. Doubleclick Ads Code was present at the URLs above, among many others. *See* Ex. 1, Edward-Elmhurst Request # 864 (intercepting communication regarding search for Dr. Julie C. Lopatka); *see also* Ex. 2 at 9-11.

78. Analytics Code was present at the URLs above, among many others. *See, e.g.,* Ex. 1, Edward-Elmhurst Request # 918 (intercepting communication regarding search for Dr. Julie C. Lopatka); *see also* Ex. 2 at 9-11.

79. Plaintiffs' pre-filing investigation did not include every subdomain of all web properties analyzed, and could not include the operation of Google Source Code prior to the date on which their investigation was conducted. Nor would it be efficient to provide the Court with the full detail of counsel's pre-filing investigation, which showed hundreds of thousands of distinct transmissions from tens of thousands of web pages. Accordingly, to the extent Plaintiffs do not present evidence regarding transmissions involving additional subdomains herein, they do not allege that such transmissions did not, in fact occur.

80. In addition, on information and belief, prior to discovery, the information Plaintiffs can show Google receives for its Ads and Analytics services from Health Care Provider web properties is under-representative of the information that Google actually receives because Google employs additional means of obtaining Health Information that are not publicly visible from a web browser. Specifically, as shown in the "Architectural Overview" of the Google Analytics Measurement Protocol diagram below, in addition to information Google obtains via a Health Care Provider's "web client" (a means through which Health Care Providers communicate online with patients, where interceptions are visible from the browser with appropriate technical tools), Google can also obtain information from the Health Care Provider's "server" directly (where communications originate and are received by the provider) which mirrors the data Google obtains directly from the web client, as well as from any mobile clients (apps) the Health Care provider uses.[15]



[15] *See Measurement Protocol (Google Analytics 4)*, GOOGLE FOR DEVELOPERS, https://developers.google.com/analytics/devguides/collection/protocol/ga4.

81. Plaintiffs were not aware of and did not consent to the collection of their Health Information by Google in any instance.

2. The Plaintiffs' Information Google Obtained Is Health Information

82. The Federal Trade Commission, which is charged with enforcing the Health Breach Notification Rule, confirms the breadth of protected information, explaining that: "Health information isn't just about medications, procedures, and diagnoses. Rather, it's anything that conveys information – or enables an inference – about a consumer's health. . . . [T]he fact that a consumer is using a particular health-related app or website – one related to mental health or fertility, for example – or how they interact with that app (say, turning "pregnancy mode" on or off) may itself be health information. . . . [L]ocation data can convey health information. For example, repeated trips to a cancer treatment facility may convey highly sensitive information about an individual's health." [16]

83. Under HIPAA, "Health information means any information . . . that: (i) [i]s created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and (ii) [r]elates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual." 45 C.F.R. § 160.103.

84. The information Google obtained concerning Plaintiffs' communications with their Health Care Providers through pages related to their medical conditions and appointments relates to their past, present, or future physical or mental health conditions. The information Google obtained when Plaintiffs interacted with their Health Care Providers' billing webpages relates to the past, present, or future payment for the provision of health care to them. The information Google obtained concerning Plaintiffs' logins to their Health Care Providers' patient portals and appointments relates to their status as patients and the provision of health care to them. The United

States Department of Health and Human Services ("HHS"), which is charged with HIPAA rulemaking and enforcement, has long recognized that patient status on its own, which is revealed when someone accesses their patient account, is protected health information.[17] The information Google Source Code intercepted from Health Care Provider web properties, including Plaintiffs' information, and transmitted to one or more Google domains invariably contains at least one value that reflects the content of communications between the website visitor (patient) and the host (Health Care Provider) relating to their health conditions, care, and/or billing.

85. The following chart lists some of the "Automatically collected," meaning default and non-optional "events" in Google Analytics, with detail regarding corresponding information obtained via Google Ads and Analytics Code. Google does not provide a straightforward public accounting of the meaning of every transmission that it receives to Ads, Doubleclick Ads, and Analytics endpoints, but by cross-referencing information available on a number of Google-authored webpages with the network traffic that Plaintiffs collected prior to filing this action, Plaintiffs are able to provide the Court with the following reference guide for interpreting the demonstrated interceptions from Plaintiffs' Health Care Provider web properties in Exs. 1 and 2.[18]

[17] *Guidance Regarding Methods for De-identification of Protected Health*, U.S. Dep't of Health and Hum. Serv. (Nov. 26, 2012), https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/De-identification/hhs_deid_guidance.pdf ("an indication that the individual was treated at a certain clinic . . . would be [protected]") (emphasis added); *see also Marketing*, U.S. Dep't of Health and Hum. Serv. (Rev. Apr. 3, 2003), https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/marketing.pdf ("covered entities may not sell lists of patients . . . without obtaining authorization from each person on the list"); 67 Fed. Reg. 53186 (Aug. 14, 2002); 78 Fed. Reg. 5642 (Jan. 25, 2013) (finding that it would be a HIPAA violation "if a covered entity impermissibly disclosed a list of patient names, addresses, and hospital identification numbers").

[18] Plaintiffs base the contents of this chart upon information in Exhibit 8, *Measurement Protocol Parameter Reference*, GOOGLE FOR DEVELOPERS/ANALYTICS, which on information and belief is no longer available online; as well as *[GA4] Campaigns and traffic sources*, GOOGLE ANALYTICS HELP, https://support.google.com/analytics/answer/11242841, *[GA4] Analytics event parameters*, GOOGLE ANALYTICS HELP, https://support.google.com/analytics/table/13594742; *[GA4] Enhanced measurement events*, GOOGLE ANALYTICS HELP, https://support.google.com/analytics/answer/9216061?hl=en&ref_topic=13367566.

Field	Value and Explanation
dl	Value: Full URL (page_location event in Analytics)
	Explanation: The "dl" (document location) field identifies the full URL of the webpage that a patient is viewing. Google acknowledges that the "dl" field and value is "content information."[19] The "dl" field and value therefore identifies and transmits the content of the patient's current communication. Google Ads, Doubleclick, and Analytics code also transmits the URL in fields labeled "url" or "oref." *See, e.g.,* Ex. 1, Gundersen Request # 694, MedStar Request # 1493, Edward-Elmhurst Request # 918.
dt	Value: The title of the page or document that is being viewed (page_title in Analytics)
	Explanation: The "dt" field (document title) equals a value that identifies the document title of the web page being viewed. Google acknowledges that the "dt" field and its value is "content information."[20] Transmission of page titles in Ads and Doubleclick Ads domains can also appear as values in the "tiba" field. *See, e.g.,* Ex. 1, Gundersen Request # 694, Kaiser Request # 1649.
dr	Value: Referring URL
	Explanation: The "dr" field equals a value that identifies the document title of the web page from which a user navigated to the current URL, which may be on the same web property as the current URL. The "dr" field and value identifies and transmits the content of a patient's specific communication. *See, e.g.,* Ex. 1, Kaiser Request # 1649, Edward-Elmhurst Request # 918.
t	Value: Event (value in Analytics)
	Explanation: The "t" field describes a particular type of event. The "t" field and value thus reflects a specific action being taken by a patient. "Events" are transmitted to Google when a website visitor takes an action on a page where Google's third-party tracking technology is deployed, such as clicking a hyperlink on the page. For example, t=pageview, t=screenview, t=event, t=transaction, t=item.[21] *See, e.g.,* Ex. 1, Gundersen Request # 568, MedStar Request # 1443, Kaiser Request # 1718, MedStar Request # 1523.
cc	Value: Attribution / Traffic Source (campaign_content in Analytics)

[19] *Id.* (Ex. 8) at 8.

[20] *Id.* at 9-10.

[21] *See How Google Analytics Collects Data*, ANALYTICS MARKET, https://www.analyticsmarket.com/blog/how-google-analytics-collects-data/; Ex. 8, *Measurement Protocol Parameter Reference*, at 7.

Field	Value and Explanation
	Explanation: The ad content that was associated with the start of a session, for example an email marketing the web property.
ck	Value: Campaign Term (campaign_term in Analytics)
	Explanation: The search term an individual used that brought them to a particular website. *See, e.g.,* Ex. 1, Gundersen Request # 830.
cs	Value: Campaign Source (campaign_source in Analytics)
	A representation of the publisher or inventory source (e.g. Facebook) from which traffic originated.
ec	Value: Event Category
	Explanation: The "ec" field provides further specificity as to the "event" (e.g. action) being taken by a patient. According to Google, this field "[s]pecifies the event category. Must not be empty."[22] For example, ec=outbound link *See e.g.,* Ex. 1, MedStar Request # 1239, Kaiser Request # 1718.

86. In addition to transmitting URLs, referring URLs, "event" information reflecting a patient's activities, and values for advertising tracking and attribution by default, Google Analytics also allows for transmission of "Enhanced measurement events," which are optional features for sending even more information about a visitor's activity to Google, such as values for "view_search_results," which tracks, as a separate category, when the URL (which Google obtains automatically) indicates that the user is viewing the results of a search they performed. On information and belief, based upon a review of Google's descriptions of enhanced measurement events, they generally categorize the information that Google automatically obtains with more granularity, breaking down for the web property owner some of the information that Google infers from the automatically collected events.

87. Google also lists a number of "recommended" events for particular industries, which are not automatically collected, and allows for creation of "custom" events, which it says

[22] Ex. 8, *Measurement Protocol Parameter Reference,* at 10.

should be created only "when no other events work for your use case." Adding enhanced, recommended, or custom events only increases the information that Google obtains (or, in many cases, the granularity with which Google *reports* what it has obtained). These events are transmitted in addition to, not in lieu of, the automatic events. Plaintiffs' Health Care Providers did not avoid the transmission of automatic events, as reflected in Exhibits 1 and 2.

88. Below is a list of additional transmission types that Plaintiffs have observed in network traffic from their Health Care Provider web properties to Google. Plaintiffs are unable to confirm from Google's documentation whether transmission types can be prevented from a web client, but can confirm that transmissions with these values, and many others, were in fact sent to Google as of approximately May 2023 from each of Plaintiffs' Health Care Provider web properties. Plaintiffs' understanding of the meaning of these additional categories of information is drawn from the document attached as Exhibit 8, which defines "parameters" that could be sent through Google's Measurement Protocol and which is attached hereto because it appears to be no longer accessible online.

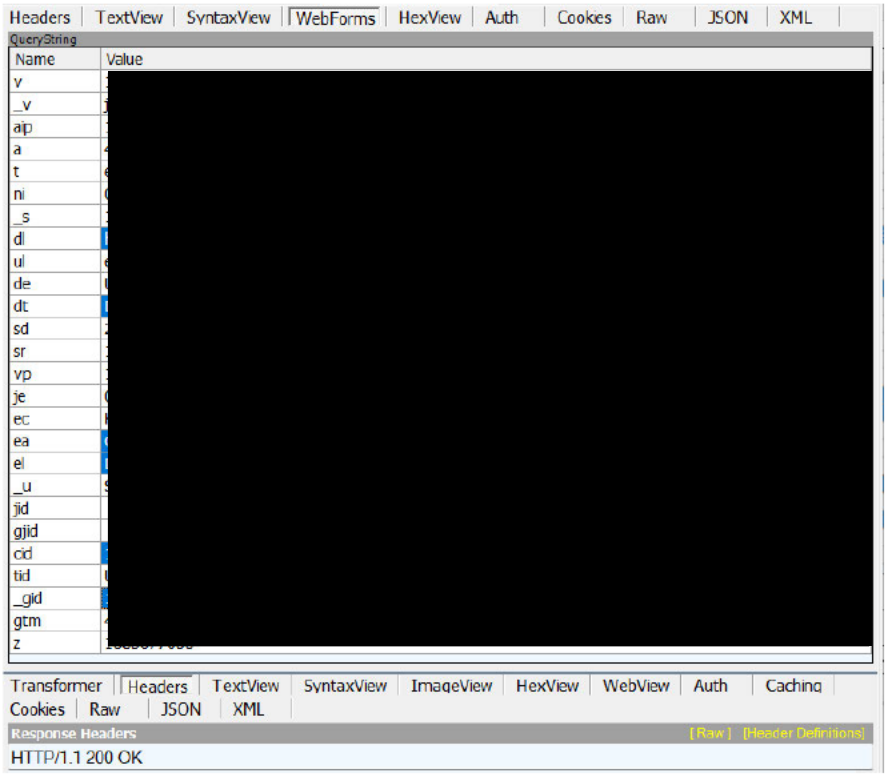
Field	Value and Explanation
ea	Value: Click
	Explanation: The "ea" field provides further specificity as to the "event" (e.g. action) being taken by a patient. According to Google, this field "[s]pecifies the event action. Must not be empty."[23] For example, ea=Clicked Request/Book Appointment/Online Button. *See, e.g.* Ex. 1, Gundersen Request # 694, Kaiser Request # 1649, Kaiser Request # 1718, MedStar Request # 1523.
el	Value: Event Label
	Explanation: The "el" field provides further specificity as to the "event" (e.g. action) being taken by a patient. According to Google, this field "[s]pecifies the event label."[24] For example, el=user_action.alter_view.request_appointment. *See, e.g.*, Ex. 1, Gundersen Request # 694, Kaiser Request # 1649, Kaiser Request # 1718, MedStar Request # 1523.

[23] *Id.* at 10-11.

[24] *Id.* at 11.

Field	Value and Explanation
ec	Value: Event Category
	Explanation: The "ec" field provides further specificity as to the "event" (e.g. action) being taken by a patient. According to Google, this field "[s]pecifies the event category. Must not be empty."[25] For example, ec=Buttons. *See, e.g.,* Ex. 1, Kaiser Request # 1718, Kaiser Request # 1649.

89. Examples reflecting the types of data collected about each Plaintiff in Exhibits 1 and 2 show that Google intercepted these values, and thus the contents of Plaintiffs' specific communications with their Health Care Provider. For example, the screenshot below reflects data intercepted by Google Analytics Code from Plaintiff John Doe I's healthcare provider, Gundersen Health, while booking an appointment with urologist Dr. Joseph Endrizzi, a urologist in La Crosse, Wisconsin:



[25] *Id.* at 10.

3. The Plaintiffs' Health Information Google Obtained Is Identifiable

90. Under HIPAA, "Individually identifiable health information" means health information as HIPAA defines that term, (i) that identifies the individual; or (ii) with respect to which there is a reasonable basis to believe that the information can be used to identify the individual. 45 C.F.R. 160.103. HIPAA's corresponding federal regulations further clarify that "health information is **not** individually identifiable health information only if" one of two things is true. Either (i) "[a] person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods" applies and documents those methods to identifiable information and "determines that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is a subject of the information;" or (ii) all actual or potential identifiers listed in the regulation, including "Web Universal Resource Locators (URLs)," "Internet Protocol (IP) address numbers" and (with an exception for a new unrelated code created solely for reidentification that is never disclosed) "[a]ny other unique identifying number, characteristic, or code" has been removed from the information. 45 CFR 164.514(b)

91. The information intercepted by Google for Ads, Doubleclick Ads, and Analytics endpoints on webpages where Google Source Code is present invariably contains at least one identifier that could—and does—identify the individual. As demonstrated in the files attached as Exhibit 1, transmissions include "Client" information, including "User-Agent" information about the device that is being used; "Cookies" information, including some of the cookies placed on the individual's device; and "Request Headers," containing a string of variables that reflect information being tracked on a web property, among other things. Google also receives the user's IP address.

a. IP Address and User-Agent

92. The user's IP address and User-Agent information are always transmitted to Google when Google Source Code is deployed.

b. Cookies

93. Google uses many classic third-party cookies to identify individuals. Classic third-party cookies transmitted from Plaintiffs' Health Care Provider web properties, and generally via the Google Source Code, include (but are not limited to) the following.

Field	Value and Explanation
DSID	Explanation: cookie is associated with a Google Display Ad (e.g., www.DoubleClick.net), and contains a value that can identify a patient's Google Account (if they have one). *See, e.g.,* Ex. 1, Kaiser Request # 405, Kaiser Request # 867, Kaiser Request # 2223, Kaiser Request # 318, Kaiser Request # 727, MedStar Request # 1493, MedStar Request # 1596, Edward-Elmhurst Request # 864.
IDE	Explanation: The IDE field is a Google cookie that Google calls a "Biscotti" cookie, which contains a unique alphanumeric value that is associated with and redirected to Doubleclick.net endpoints. The alphanumeric value uniquely identifies the specific browser on the patient's specific device. Google collects Biscotti cookies at the same time that it collects Google Account cookies, rendering Google reasonably capable of associating a Biscotti cookie with each Google Accountholder's Google Account information. *See, e.g.,* Ex. 1, Gundersen Request # 720, Kaiser Request # 405, Kaiser Request # 867, Kaiser Request # 2223, Kaiser Request # 318, Kaiser Request # 727, MedStar Request # 1493, MedStar Request # 1596, Edward-Elmhurst Request # 864.
NID	Explanation: The NID field is a Google cookie that Google calls a "Zwieback" cookie, which contains a unique alphanumeric value that is associated with and redirected to Google.com (Google Ads) endpoints. The alphanumeric value uniquely identifies the specific browser on the patient's specific device. Google collects Zwieback cookies at the same time that it collects Google Account cookies, rendering Google reasonably capable of associating a Biscotti cookie with each Google Accountholder's Google Account information. *See, e.g.,* Ex. 1, Gundersen Request # 722, Kaiser Request # 417, Kaiser Request # 875, Kaiser Request # 611, MedStar Request # 1504, MedStar Request # 1236, Edward-Elmhurst Request # 895, Edward-Elmhurst Request # 918.
Secure-3PSID Secure-3PAPISID Secure-3PSIDCC	Explanation: cookies that Google calls Gaia cookies, which contains a unique alphanumeric value that is associated with and redirected to Google.com on Health Care Provider web-properties and which is used to identify a person's Google Account. *See, e.g.,* Ex. 1, Gundersen Request # 722, Kaiser Request # 417, Kaiser Request # 875, Kaiser Request # 611, MedStar Request # 1504, MedStar Request # 1236, Edward-Elmhurst Request # 895, Edward-Elmhurst Request # 918.

c. GET and POST Request Headers with Disguised Google Cookies

94. In addition to classic third-party cookies, Google designed the Google Source Code to transmit additional cookies within the Request Header transmissions. This is because, beginning no later than 2018, companies that compete in the Internet browser market (such as Apple Safari and Mozilla Firefox) began blocking the third-party cookies that, until that point, were the primary method through which surveillance companies like Google tracked user communications across the web.

95. In response to efforts by Apple and Mozilla to block tracking, surveillance companies (including Google) began developing methods to track users through first-party cookies as well. That way, even if a user had blocked third-party cookies, they would still be tracked through the first-party cookies and a process called "link decoration."[26]

96. For Google Analytics and Google's associated Ads products (www.google.com and www.doubleclick.net), Google Analytics sets cookies named _ga, _gid, and _gcl_au as putative "first-party" cookies when a patient visits a Health Care Provider web property and then commands the patient's browser to re-direct the value of those cookies to Google in GET or POST requests through "link decoration" via URL "parameters" named cid and gid within the Request Headers.

97. Google's disguised third-party cookies are not recorded under "Cookies" in Exhibit 1. Instead, they are transmitted as values within the Request Headers, meaning they are visible in, and throughout, both of the relevant exhibits. As those documents show, disguised cookies transmitted from Plaintiffs' Health Care Provider web properties, and generally via the Google Court Code, include (but may not be limited to) the following:

Field	Value and Explanation
cid	Explanation: According to Google, the cid field "identifies a particular user, device, or browser instance. . . . The value of this field should be a random UUID

[26] *See WTF is link decoration?*, DIGIDAY (May 16, 2019), https://digiday.com/marketing/wtf-link-decoration/.

Field	Value and Explanation
	(version 4) as described in http://www.ietf.org/rfc/rfc4122.txt."[27] Google cid is usually the clientID identifier of the Google Analytics cookies, including the _gcl, _au, and other cookies. They are used to identify unique users and browsers and used in server-side sessionalization at Google, as well as for conversion tracking purposes.
gid	Explanation: this is a unique identifier assigned to a user on a single website when the user is logged in to a Google service in the same browser with which they are accessing the website. When this condition is true it will be assigned to the user, stored in a first-party cookie, and collected in all Google Analytics hits. If the user has Ads Personalization enabled in their Google account, this ID is used to associate pages viewed and actions taken with the user to enhance targeting and personalization by Google. When a website has Google Signals enabled in their Google Analytics property, this ID and associated data is used to enhance the audience creation and demographics reporting available to the website owner in Google Analytics.[28]
auid	Explanation: According to Google, the auid ("Advertiser user ID) is associated with a "sitewide tag," and "store a unique identifier for a user or the ad click that brought the user to your site. Then, when the same tags fire on the conversion page, it will use the stored GCLID and AUID to properly measure conversions."[29]

98. Google Analytics sets the _ga, _gid, and _gcl_au cookies as putative "first-party cookies" on *every* property where Google Analytics source code appears and commands users' browsers to re-direct the value of those ghost-cookies to Google in a GET or POST request via the cid and gid parameters for *every* communication that occurs on those properties where Google Analytics source code is present. Thus, with respect to this case, Plaintiffs allege the following Who, What, When, Where, Why, and How for Google's deployment of "ghost cookies":

a. Who: Google and the employees in charge of Google Ads and Analytics, including its engineers like Steve Ganem;

b. What: The _ga, _gid, _gcl_au cookies; and the cid and gid parameters through which the _ga, _gid, and _gcl_au cookie values are re-directed to Google;

[27] Ex. 8, *Measurement Protocol Parameter Reference,* at 5.

[28] *GDPR and Google Analytics: Is It Really Illegal?*, INFOTRUST (Jan. 20, 2022), https://infotrust.com/articles/gdpr-and-google-analytics-is-it-really-illegal/#:~:text=Google%20Analytics%20ID%20(_gid)%20%E2%80%93%20this%20is%20a%20unique%20identifier,they%20are%20accessing%20the%20website.

[29] *Troubleshoot your sitewide tagging*, GOOGLE ADS HELP, https://support.google.com/google-ads/answer/9148089?hl=en

c. When: Every time a patient exchanges a communication at a Health Care Provider web property where at-issue Google Source Code is present;

d. Where: Every page of every Health Care Provider web property in the United States where Google Source Code is deployed, including Plaintiffs' Health Care Providers' web properties and the more than 5,000 such properties that Plaintiffs specifically identified to Google in or around July 2023;

e. Why: To evade cookie blocking technologies to ensure that Google Analytics and its other properties work regardless of the browser that someone is using;

f. How: By designing the Google Source Code so that it implants Google cookies as "first-party" cookies on non-Google websites even though they are actually Google cookies and then commands web-browsers to re-direct the values for those cookies to Google's servers through GET and POST requests via link decoration.

99. Examples reflecting the data collected from Plaintiffs' Health Care Providers in Exhibit 1 further show that Google intercepted these Identifiers with the contents of specific communications. For example, the sample screenshot in Paragraph 89 shows that Google Analytics Code transmitted a cid/ga and _gid Identifier with the information intercepted about the specific event reflecting the booking of an appointment with a urologist at Gundersen. These Identifiers uniquely distinguish all patients affected (including Plaintiffs) from other visitors to the same web property, and to Google specifically, within Google's systems.

100. Google intercepts these identifiers with the value fields described above, contemporaneously with the visitor's interaction with a Health Care Provider's website through what is known as a "POST" or "GET" request. Per HTTP standards, successful requests—*i.e.*, those that reach and are accepted by their target endpoint—are acknowledged with a response code of "200", which confirms receipt by the targeted endpoint. Google confirmed receipt of the intercepted data from each Plaintiff's Health Care Provider with an HTTP 200 code.

101. The information intercepted by each Google Ads, Doubleclick Ads and Analytics Source Code which cause the Health Information intercepted to be identifiable is summarized as follows:

Patient Identifier	Ads	Doubleclick Ads	Analytics
Google Account	✓	✓	✓
ga cookie / cid	✓	✓	✓
gid cookie / _gid	✓	✓	✓
Event Join IDs	✓	✓	✓
NID cookie	✓		
IDE cookie		✓	
Device ID	✓	✓	✓
IP address	✓	✓	✓
User Agent	✓	✓	✓
Device Properties	✓	✓	✓
Content	✓	✓	✓
Button Clicks			✓
Communications, including Searches, and Requests for Specific Information about Doctors, Conditions, Diseases, Patient Portals, Appointments	✓	✓	✓

102. The cookies and IP addresses obtained in connection with transmissions via Google Ads and Analytics Code are themselves independently sufficient to render each transmission "Individually identifiable health information" pursuant to HIPAA regulations.

103. The transmissions cannot be excluded from the definition of Individually identifiable health information because Google, the recipient, at all times maintains records that enable it to associate the various identifiers it obtains with other identifiers, and ultimately with an individual's Google Account ID (known as a "GAIA" id) which is associated with their name and contact information.

104. This holds true even for individuals who are not signed into any Google Account at the time of transmission because Google correlates the signed-out browser identifying cookies for Google Analytics (gcl, au), Google Ads Endpoints (NID), and Google Doubleclick Ads Endpoints (IDE), among other products, with individuals' Google Accounts, and their contents, any time that Google collects the signed-out browser identifying cookie.

105. Google's ability to identify the individuals to whom the transmissions pertain is also evident in the "Google Signals" program, which provides Health Care Providers with the option to "better understand your customers across devices using Google's signed-in data." [30] To do this, Health Care Providers need only click a button to "activate" Google Signals, thereby "updating" the "existing Google Analytics features" in their accounts "to also include aggregated data from Google users who [according to Google] have consented to Ads Personalization."[31] With Google Signals activated, Health Care Providers can "serve ads in Cross Device-eligible remarketing campaigns" (meaning they can target people on the basis that they visited the Health Care Provider's web property on devices other than the ones used to do so, discussed in Section V(E), *infra*).[32] By definition, Google could not link Analytics data to "signed-in data" (which is categorized for storage linked to Google Account Holders' names and direct contact information) if the Analytics data were not, itself, identifiable.

106. Google also maintains a data system with "proto files" that "shows that Google commingles signed-in and signed-out information" together in various columns that identify specific individuals. One such column involves co-mingling data that includes, but are not limited to, several unique identifiers: GAIA ID, Biscotti ID, Zwieback ID, PPID, Device ID, First Party User IDs, Buyside Publisher ID, Publisher User IDs, DUIS, YouTube Visitor ID, precise geo-coordinates, areas-of-interest, shipping address, credit card information, household income, age, gender, race, ethnicity, children, and education.

107. Google also maintains numerous files that contain GAIA, Biscotti, and/or Zwieback alongside each other or with other "identifier[s] that can be used to bridge Gaia, Biscotti, and Zwieback ID spaces," such as device IDs like an Android ID or iOS IDFA; or contain "high entropy fields, which when combined together could be sufficient to uniquely identify users

[30] *Activate Google signals*, GOOGLE ANALYTICS HELP, https://support.google.com/analytics/answer/7532985.

[31] *Id.*

[32] *Id.*

alongside GAIA, Biscotti, or Zwieback," including "fields [i.e. information categories] representing various types of fingerprints to uniquely identify users" such as browser-fingerprinting, Picasso fingerprinting, and font fingerprinting.[33]

108. A Google employee has publicly stated that Google maintains tables that "contain mappings between Google Analytics User ID (UID) or client ID (CID) and Biscotti" as well as "mappings between UID or CID and device ID received from App events." This document was filed in this action at Dkt. 61-4. Google acknowledges that it maintains associations between the various Google products that obtain information about a user's browser.[34]

109. The identifiers described above show that: (i) information Google intercepts from Health Care Provider web properties, including those visited by Plaintiffs, are associated with individual users and their devices; (ii) that the identifiers on their own can identify a unique individual; and (iii) that Google can combine those identifiers with other information in its possession, to further associate the data intercepted from Health Care Providers with profiles it maintains about that specific individual.

D. Google's Acquisition of Class Members' Health Information

110. Google's acquisition of Health Information from the Gundersen, Kaiser, TMH, MedStar, Shannon Medical, and Edward-Elmhurst Health Web Properties discussed above reflects and represents a pervasive problem affecting patient privacy throughout the United States.

1. Google Source Code Is Extensively Integrated on Class Members' Health Care Provider Websites

111. Unrecognized by patients and relevant authorities, Google Source Code and integrated Ads and Analytics usage quietly proliferated for years across and within Health Care Provider web properties until, by 2023, it was operating on up to 91% of such properties nationwide.

[33] *See* Dkt. 61

[34] *Remarketing Lists for Search Ads with Analytics*, GOOGLE ANALYTICS HELP, https://support.google.com/analytics/answer/6212951.

112. Public health authorities became aware that this was a nationwide problem in or around April 2022, when a team of researchers from the Department of Electrical and Computer Engineering at the University of Illinois at Urbana-Champaign contacted HHS about the issue. Email correspondence dated April 22, 2022, shows that the researchers shared findings concerning "information leaks to third parties on Web sites that display individual health information," which was focused "on two categories of web sites: hospitals that use MyChart patient portals powered by Epic (a healthcare software company) and telehealth web sites."[35] Within that subset of Health Care Provider web properties (which included Edward Elmhurst Health), the researchers explained they had "found 60 MyChart patient portals that use Google Analytics or Facebook Pixel to track visitors on their login pages" sending "the URLs and titles of the pages that patients visit, such as 'Health Record: Blood Pressure', to Google and Facebook respectively."[36] The researchers noted that cookies associated with the information "makes the health information transmitted to Google and Facebook identifiable."[37]

113. Concurrently with research at the University of Illinois, reporters and technologists at non-profit news organization "The Markup" worked to inform the public. They conducted an investigation focused on the Facebook Pixel, and on June 16, 2022, reported that "33 of Newsweek's top 100 hospitals in the country [were] sending sensitive data to Facebook via the pixel . . . as of June 15, 2022."[38] Additional research and reporting followed. For example, on or around September 12, 2022, JAMA Internal Medicine published research concerning the prevalence of third-party tracking technology on abortion clinic websites, the findings of which

[35] Ex. 4, April 22, 2022 email correspondence with Gordon-Nguyen, Marissa (HHS/OCR), *Am. Hospital Ass'n v. Becerra*, No. 23-cv-01110-P, Dkt. 49-8.

[36] *Id.*

[37] *Id.*

[38] Todd Feathers et al., *Facebook Is Receiving Sensitive Medical Information from Hospital Websites*, THE MARKUP (June 16, 2022), https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites.

suggested "that 99.1% of US based abortion clinic web pages include third-party tracking," and that the most prevalent tracking entity was Google (97.3%), followed by Meta with 85%.[39]

114. As a general rule, when Google Source Code appears on a single page of a web property, it also appears on *every* other page of that web property such that Google rarely (if ever) collects only the "homepage" of a property. This is by design. Google urges all developers to place the Google Source Code in the "header" of its HTML so that Google's commands to re-direct a person's identifiers and communications content are implemented before the website's own communication with the person is complete and on every single page to ensure maximum tracking.

115. The only potential exception of which Plaintiffs are aware is where the Google Source Code intercepts every page at a Health Care Provider's property and logins/logout to the patient portal, but not communications inside the patient portal. In the absence of discovery, Plaintiffs cannot state the percentage of patient portals for which Google also intercepted all communications inside the patient portal. However, Plaintiffs are aware and allege that *Google intercepted inside-the-portal communications for every patient portal in the United States associated with Cerner* (a major patient portal vendor) including the MyMedStar patient portal. In addition, as researchers at the University of Illinois concluded, Google intercepted inside-the-portal communications for a large number of patient portals associated with Epic (the other major patient portal vendor), including the patient portal at Edward Elmhurst.

2. HHS Recognized Google's Third-Party Tracking Technologies Are a Nationwide Privacy Problem

116. Not long after receiving the research findings from the University of Illinois, HHS issued a bulletin in December 2022 reminding covered entities that they "are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI to tracking

[39] Ex. 5, Ari B. Friedman, et al., *Prevalence of Third-Party Tracking on Abortion Clinic Web Pages*, JAMA (Sept. 8, 2022), at 274-275, https://jamanetwork.com/journals/jamainternalmedicine/fullarticle/2796236.

technology vendors or any other violations of the HIPAA Rules."[40] This guidance was amended in March 2024 to clarify that not every transmission from every webpage on a Health Care Provider website necessarily results in impermissible disclosures (e.g. some pages might not require users to enter health information), and to reaffirm that the allowable use of third-party tracking technology is, nonetheless, extremely limited. It provided that, for information within user-authenticated webpages such as "patient portal" pages that "generally have access to PHI," any third-party tracking must be configured "to **only** use and disclose PHI in compliance with the HIPAA Privacy Rule."[41]

117. As for "unauthenticated" webpages, which can be accessed by patients and non-patients alike, the guidance provides that Health Care Providers can utilize tracking technology on pages that relate only to issues other than physical or mental health or conditions, the provision of health care, or payment for the provision of health care, "such as a webpage with general information about the regulated entity like their location, visiting hours, employment opportunities, or their policies and procedures."[42] Other types of unauthenticated webpages, such as "a hospital's webpage listing its oncology services" contain protected Health Information when an individual accesses them for purposes related to their own conditions, treatment, or care, but not when they are accessed for purposes unrelated to healthcare, such as conducting research for a term paper. [43]

[40] Ex. 6, *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates*, U.S. Dep't of Health and Hum. Serv. (Dec. 1, 2022), https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html#ftnref22. That HHS considered the research and communications referenced above is reflected in their inclusion within the Index to the Administrative Record that HHS submitted in connection with legal challenges to the December 2022 Bulletin, attached hereto as Exhibit 7.

[41] *Id.* (emphasis original).

[42] *Id.*

[43] *Id.* The Guidance was amended again in June 2024 to reflect a court order vacating the portion of the Guidance requiring covered entities to prevent the transmission of all IP addresses with all domains that *could* relate to a visitor's health on the basis that some such transmissions, *e.g.*, those involving a hypothetical student interacting with a Health Care Provider for research purposes, would not contain Health Information due to the nature of the visit. *See id.*; *see also Am. Hosp. Ass'n v. Becerra*, No. 4:23-CV-01110-P, 2024 WL 3075865, at *17 (N.D. Tex. June 20, 2024).

3. Plaintiffs' Investigation Confirms that Google's Third-Party Tracking Technologies Are a Nationwide Privacy Problem

118. Despite HIPAA's requirements and HHS's guidance specific to third-party tracking technology, Google Source Code on Health Care Provider web properties is typically configured to transmit protected health information to Google. Prior to filing this action in 2023—two months after HHS issued its reminder—Plaintiffs' counsel analyzed 5,297 Health Care Provider web properties, and noted browser-based transmissions still going to Google Ads Code endpoints on 59 percent of the web properties analyzed; transmissions to Google Doubleclick Ads Code endpoints on 50 percent; and transmissions to Google Analytics code endpoints on 60 percent, as well as code indicating use of the Google Tag Manager, *i.e.* the Google Tag and potentially other entities' tags, on 67 percent of the websites.

119. The interceptions identified by Plaintiffs identified transmissions on a large number of webpages, including many that obviously relate to patient health. To provide specific examples, Google intercepted communications and obtained other Health Information through its Ads Code, from:

https://my.njhealth.org/PatientPortal/Users/Login.aspx
https://www.eastgeorgiaregional.com/hospital-patient-portal
https://www.havasuregional.com/patient-portal
https://mychart.atlantichealth.org/MyChart/Authentication/Login?
https://www.holycrosshealth.org/mychart/
https://franciscanbeaconhospital.org/mychart-at-franciscan-beacon-hospital/
http://aultmanorrville.org/Aultman-Hospital-Information/find-a-physician/findaphysician.aspx
http://utmc.utoledo.edu/ut-medical-center/billing/index.html
https://abqhospital.com/clinical-services/
https://zucker.northwell.edu/patient-information
https://www.yumaregional.org/services/rheumatology/

120. Google intercepted communications and obtained other Health Information through its Doubleclick Code, from:

https://www.maryfreebed.com/make-an-appointment/
https://www.jeffersonhealth.org/appointment-

Plaintiffs here, of course, are patients of their respective Health Care Providers, and bring this action on behalf of patients of Health Care Providers regarding transmissions of identifying information about users who *are* visiting the webpage for their healthcare needs which all parties and the Court in *Am. Hosp. Ass'n* agreed is Health Information. *See* 2024 WL 3075865, at *13.

request?refUrl=https://www.jeffersonhealth.org/conditions-and-treatments?search-query=
https://my.njhealth.org/PatientPortal/Users/Login.aspx
https://dallascohospital.followmyhealth.com/Login/Home/Index?authproviders=0&returnArea=PatientAccess#!/default
https://danctrigg-memorial-hospital.phs.org/Pages/default.aspx
https://coffeeregional.followmyhealth.com/Login/Home/Index?authproviders=0&returnArea=PatientAccess#!/default
https://chmccook.followmyhealth.com/Login/Home/Index?authproviders=0&returnArea=PatientAccess#!/default

121. Google intercepted communications and obtained other Health Information through its Analytics Code, from:

https://www.nkch.org/patients-and-guests/for-patients/before-your-visit/schedule-an-appointment
https://www.kennedykrieger.org/patient-care/preparing-for-your-appointment-admission/make-an-appointment/insurance-billing-and-payment/online-bill-pay
https://www.kentri.org/services/cancer/lung-health-clinic
https://www.kellwest.com/medical-records
https://www.umiamihealth.org/en/sylvester-comprehensive-cancer-center
https://www.keckmedicine.org/conditions-and-treatments/
https://www.uhd.org/index.php/providers
https://www.kch.org/gynecology
https://www.kauhospital.org/patients-and-visitors/patient-guide/insurance-and-billing/
https://www.kansashealthsystem.com/records-requests
https://my.peacehealth.org/MyPeaceHealth/Authentication/Login?

122. Plaintiffs' findings, namely that Google's interception of communications on Health Care Provider web properties is commonplace, are consistent with the findings of researchers at the University of Illinois at Urbana-Champaign who contacted HHS about this widespread privacy issue. In the vast majority of cases, when deployed, Google's third-party tracking technologies are deployed on every page of a web property and collect every communication thereon, consistent with Google's guidance to install its tag on every page of the website. Even if and to the extent third-party tracking ever occurs solely on the home landing page of a particular Health Care Provider's web property, a patient's actions on the homepage can and often do, themselves, reveal Health Information, such as the visitor's patient status when they click to log into a patient portal from the landing page, the contents of the searches they perform in search bars, which are generally if not universally present on a landing page in light of their

function (i.e., to facilitate navigation of a website to relevant subdomains), and information pertaining to their conditions when they click links presented on a homepage to other pages regarding those conditions.

E. Google's Use of Plaintiffs' and Class Members' Health Information

123. When Google intercepted Health Information from Plaintiffs' Health Care Providers, it did far more with the information than store it for the web property owner's analysis.

124. In the vast majority of cases, as discussed above with respect to Google Services, even data collected via Google Analytics is linked or integrated with other advertising systems, which are a primary driver of Google's revenues from the Google Services segment of its business. This integration occurred for each of Plaintiffs' Health Care Providers, evidenced by transmissions from their web properties to Google Ads and Google Doubleclick Ads endpoints, in addition to Google Analytics as set out above. This integration occurred on most Health Care Provider web properties that used Google Analytics, evidenced by the presence of Ads *and* Analytics Code on thousands of web properties. This integration occurred so that Health Care Providers could use Google Analytics to "reach" patients and potential patients to exchange health information, as the American Hospital Association ("AHA") admits in a 2023 letter on behalf of nearly 5,000 health care organizations.[44]

125. Whether or not such integration occurs, the data transmitted to Google—including Health Information—is received, categorized, and processed by Google. Except in the extremely rare case where a Health Care Provider *only* transmitted data to Google Analytics endpoints, *and* disabled and opted out of a large number of Google Analytics features which Google enables by default and encourages its customers to use, Google also uses the content it intercepts for a number

[44] *AHA Letter to OCR on HIPAA Privacy Rule, Online Tracking Guidance*, AM. HOSP. ASS'N (May 22, 2023), https://www.aha.org/lettercomment/2023-05-22-aha-letter-ocr-hipaa-privacy-rule-online-tracking-guidance (arguing that "many hospitals had made the reasonable choice of working with Google to reach more consumers with better-designed websites and better-presented health information").

of purposes directly and indirectly supporting Google's business interests including, but in no way limited to, third-party advertising.

126. Insofar as Google posts policies restricting particular advertising uses of the information Google intercepts from web properties it categorizes as relating to health, and insofar as Google may enforce those policies in some circumstances, the policies do not restrict *Google's* receipt, categorization, and processing of the information by their terms, or in practice. At most, they concern only a limited subset of uses by health-related entities. Google has no policy or intention to restrict its own access to, and use of, Health Information for other business purposes beyond those expressly identified in its policies.

1. Google uses Health Information to Classify Individuals, Web Properties, and Internet Browsing Activities

127. At the outset, Google processes each transmission from each Health Care Provider web property in the same way it processes transmissions from all other web properties in which Google Source Code is embedded. This processing includes categorizing the data using "Content Taxonomy" standards the same or similar to those published by the Interactive Advertising Bureau (IAB), which include the following categories: medical health, blood disorders, bone and joint conditions, brain and nervous system disorders, cancer, dental health, diabetes, digestive disorders, ENT conditions, endocrine and metabolic diseases, hormonal disorders, menopause, thyroid disorders, eye and vision conditions, foot health, heart and cardiovascular diseases, infectious diseases, lung and respiratory health, mental health, reproductive health, birth control, infertility, pregnancy, sexual health, skin and dermatology, sleep disorders, substance abuse, medical tests, pharmaceutical drugs, surgery, and vaccines. Google has publicly listed categories or "verticals" that it uses to categorize the content of web properties and their associated transmissions[45] and includes (among others) the following health categories:

Criterion ID	Parent ID	Category
45	0	/Health
624	623	/Health/Aging & Geriatrics/Alzheimer's Disease

[45] *Verticals*, GOOGLE ADS API, https://developers.google.com/google-ads/api/data/verticals.

Criterion ID	Parent ID	Category
499	45	/Health/Alternative & Natural Medicine
625	419	/Health/Health Conditions/AIDS & HIV
628	419	/Health/Health Conditions/Arthritis
630	419	/Health/Health Conditions/Blood Sugar & Diabetes
429	419	/Health/Health Conditions/Cancer
571	419	/Health/Health Conditions/Eating Disorders
1329	1328	/Health/Health Conditions/Endocrine Conditions/Thyroid Conditions
638	419	/Health/Health Conditions/GERD & Digestive Disorders
643	559	/Health/Health Conditions/Heart & Hypertension/Cholesterol Issues
641	942	/Health/Health Conditions/Neurological Conditions/Learning & Developmental Disabilities
642	641	/Health/Health Conditions/Neurological Conditions/Learning & Developmental Disabilities/ADD & ADHD
1856	641	/Health/Health Conditions/Neurological Conditions/Learning & Developmental Disabilities/Autism Spectrum Disorders
818	419	/Health/Health Conditions/Obesity
631	819	/Health/Health Conditions/Pain Management/Headaches & Migraines
627	824	/Health/Health Conditions/Respiratory Conditions/Asthma
420	419	/Health/Health Conditions/Skin Conditions
1353	1352	/Health/Medical Devices & Equipment/Assistive Technology/Mobility Equipment & Accessories
639	437	/Health/Mental Health/Anxiety & Stress
640	437	/Health/Mental Health/Depression
645	45	/Health/Pediatrics
647	195	/Health/Reproductive Health/Infertility
202	195	/Health/Reproductive Health/Male Impotence
421	195	/Health/Reproductive Health/Sexually Transmitted Diseases
1350	257	/Health/Substance Abuse/Drug & Alcohol Treatment
1235	257	/Health/Substance Abuse/Steroids & Performance-Enhancing Drugs
1503	246	/Health/Vision Care/Laser Vision Correction
648	45	/Health/Women's Health

128. Google uses the output of its categorization algorithms such as (but not limited to) the example above to create "segments" of individual website visitors based upon their actions (visiting a webpage in a particular categorization), or their "affinity," meaning "habits and interests," among other categorizations.[46] Google builds and maintains these profiles in its systems for a variety of uses.

[46] *About audience segments,* GOOGLE ADS HELP, https://support.google.com/google-ads/answer/2497941.

2. Google Admits to Making Multiple Uses of Health Information

129. Google admits to using "information from sites or apps that use our services," *i.e.* data obtained via Google Ads and Analytics, in a variety of ways. Google does not purport to prohibit (or refrain from) using Health Information in every undertaking for which it uses the data, although it certainly leaves the reasonable reader of its policies with that impression. What Google actually says, while distracting with numerous incorporated pages and references to "ads," is that in addition to using "information from sites or apps" for the service of personalized "ads you see on Google and [its] partners' sites and apps" (for which Google does have policies relating to use of Health Information it collects), Google also uses this information to create personalized "content" on Google and its partners' sites and apps, as well as "to deliver [Google's] services, maintain and improve them, develop new services, measure the effectiveness of advertising, and protect against fraud and abuse."[47]

130. Google unilaterally amends its policies on a routine basis. It has amended its Privacy Policy no fewer than 31 times since February 25, 2015, including seven times since this action was filed.[48] Despite the overall impression from its policies throughout that time, in all of them Google carefully avoids stating that sensitivity classifications limit Google's collection or use of information for its own purposes (*e.g.*, personalizing content) *except* potentially in the context of personalized "ads," and creating "ad profile[s]" from the data—a narrow subset of uses. As discussed below, even those limitations are circumscribed to direct use in particular advertising products, and do not prohibit (let alone prevent) all profiling or all uses of Health Information in

[47] Google's Terms of Service contain similar admissions. *See* Ex. 9, *Terms of Service*, GOOGLE PRIVACY & TERMS, at 12 (Jan. 5, 2022), https://policies.google.com/terms/archive/20220105 ("you can expect" that Google is "constantly developing new technologies and features to improve [its] services, including through use of "artificial intelligence and machine learning").

[48] *See Updates: Privacy Policy*, GOOGLE PRIVACY & TERMS, https://policies.google.com/privacy/archive?hl=en-US (archived versions of Google's Privacy Policy). Google also amended its January 5, 2022 Terms of Service on or around May 22, 2024, adding, among other things, that "If you close your Google Account and then access or use our services without an account, that access and use will be subject to the most current version of these terms." *See* https://policies.google.com/terms/archive/20220105-20240522?hl=en (showing recent modifications). Google did not amend the acknowledgement regarding AI noted above.

all advertising. Google acknowledges that whether or not information is included in a person's "ad" profile, or used to "personalize the ads Google shows to you," it "can still be used for the other purposes mentioned above."[49]

131. Until May 15, 2023, Google expressly incorporated these admissions into the Google Analytics Terms of Service, a contract of adhesion between Google and entities using Google Analytics which Google calls "publishers." Google has used at least three versions of the contract, dated June 17, 2019, amended March 31, 2021, and most recently amended May 15, 2023.[50] As it appeared in 2019 and 2021, the contract provided that "Google and its wholly owned subsidiaries may retain and use, subject to the terms of its privacy policy (located at https://www.google.com/policies/privacy/), information collected in Your use of the Service," where the incorporated policy contains the admissions discussed above.[51] Google's May 15, 2023 amendment did not reflect any change in Google's practices; the admissions themselves are still part of Google's overarching Google Terms of Service.

a. Google Uses Health Information for Advertising

132. With respect to advertising, Google encourages all Google Analytics customers to use Google's segments to advertise their products and services, including to "[c]reate remarketing audiences from your Google Analytics data, and share those audiences with your linked advertising accounts."[52] Google currently brands its "remarketing" options (i.e., targeting past

[49] *Id.* Google used the Health Information it intercepted from Plaintiffs' and other Class members' Health Care Providers for these and other "advertising" purposes as discussed further below.

[50] *See Google Analytics Terms of Service*, GOOGLE MARKETING PLATFORM (May 15, 2023), https://marketingplatform.google.com/about/analytics/terms/us/. Two prior versions, dated March 31, 2021 and June 17, 2019, respectively, are available from hyperlinks at the bottom of the webpage.

[51] *See id.*

[52] *Activate Google signals for Google Analytics 4 properties*, ANALYTICS HELP, https://support.google.com/analytics/answer/9445345. *See also About Your Data Segments for Search Ads*, GOOGLE ADS HELP, https://support.google.com/google-ads/answer/2701222.

visitors or customers of a website on the basis of their visit or a particular action) as a component of "your data segments," with the same general functionality.[53]

133. Health Care Providers are Google Analytics customers. As explained above, the AHA announced that "many" of its members use Google Analytics to "reach" consumers with health information and attract patients. Google Ads Code is prevalent on Health Care Provider web properties, suggesting that the AHA is correct. Nonetheless, Google purports to prohibit "[a]dvertisers promoting products and services that fall within sensitive interest categories" (which, on information and belief, can include Health Care Providers attempting to reach consumers with health information), from using "advertiser-curated audiences" for their advertising campaigns.[54] Google has many reasons, discussed in Sections V(E)(2)(b)-(c) and V(F), below, not to enforce that policy. Insofar as it is enforced, the impact falls on advertisers (Health Care Providers), not Google. They would be "unable to use" Google's remarketing features specifically to target an individual solely on the basis that the individual previously interacted with a specified page, or took a specified action, on their website.[55]

134. Google acknowledges that none of its prohibitions regarding the use of Health Information for personalized advertising impact its data collection. In its Google Analytics Advertising Features policy, incorporated into the Google Analytics terms of service, for example, Google confirms that it has no policy against the collection (*i.e.*, interception by Google) of "sensitive" information, and only claims to restrict particular uses (by advertisers) after Google has received it: "[i]f you use Google Analytics to collect sensitive information about your visitors [which Google knows and authorizes], as described in the Google Ads sensitive category

[53] *About Your Data Segments*, GOOGLE ADS HELP, https://support.google.com/google-ads/answer/2453998.

[54] *Personalized Advertising*, GOOGLE ADVERTISING POLICIES HELP, https://support.google.com/adspolicy/answer/143465?hl=en#:~:text=Advertisers%20promoting%20products%20and%20services,inadvertently%20used%20for%20targeting%20audiences.

[55] *Policy requirements for Google Analytics Advertising Features*, GOOGLE ANALYTICS HELP, https://support.google.com/adspolicy/answer/143465?hl=en#:~:text=Advertisers%20promoting%20products%20and%20services,inadvertently%20used%20for%20targeting%20audiences.

restrictions, you may not use Google Analytics to collect data *for the purpose of interest based advertising*."[56] This is not a ban on collection (transmission to Google); it allows "us[ing] Google Analytics to collect sensitive information," but advises that Google has policies to limit advertisers' use of that data for one of many "purpose[s]" Google Analytics is designed to achieve. Even assuming robust enforcement, this, at best, would limit the Health Care Providers' use of the information Google intercepts from their web properties but have no impact on Google's collection or use of the same data.

135. To the extent Health Care Providers are actually prevented from using the data Google obtains to run remarketing campaigns for their services,[57] the "segments" nonetheless already exist in Google's systems and are used for other purposes by Google, including other advertising purposes, except in extremely rare circumstances: If (unlike any of Plaintiffs' Health Care Providers) a Health Care Provider were to have *only* Google Analytics on their web property, they would have the option to turn "off" a number of settings that Google encourages them to keep "on" and potentially limit the scale of Google's use of the Health Information intercepted from their web properties. These settings are the "Google products & services" setting (under threat of losing improvements to "the Google Ads system tools that you use"); the "Modeling contributions & business insights" setting (under threat of losing "better tools and [] guidance that can help your marketing and analysis efforts"); the "Technical support" setting (under threat of losing "help [to] resolve technical issues"); and the "Recommendations for your business" setting (under threat of losing "help [to] make the most of Google products"). Turning off all settings is only theoretically meaningful for Health Care Providers using only Google Analytics because the settings do not control interceptions via Google Ads Code and Google's associated uses in those systems, which Google acknowledges when describing its "business insights" setting: "When you turn this setting

[56] *Id.*

[57] On information and belief, for some or all of the time that Google's website tracking technology has been embedded in Health Care Provider websites, Health Care Providers, including Plaintiffs', were in fact able to use Google's remarketing feature.

OFF, data can still flow between Analytics and the other Google products that are explicitly linked to any of your account properties." [58] With that caveat, however, Google says that "If all settings are OFF, your Analytics data is only used to provide and maintain the Analytics service."[59]

136. As pertains to Plaintiffs' Health Information, as well as that of millions of other Class members, Google uses the information for several advertising purposes, including Google's Target CPA (target cost-per-action) bidding program, which is an automated bidding strategy that sets bids to obtain as many "conversions" (specific actions that an advertiser seeks to track) as possible. [60] Target CPA accomplishes the automatic bidding for Google's advertising clients by evaluating the "contextual signals" available to Google: "Google Ads can optimize Search, Display, and Hotel bids based on which remarketing list someone belongs to. Search and Display can also account for how recently a user was added to that list. Search also takes into account each list a user is on for a given campaign or ad group."[61] On information and belief, whether or not the "segments" represented in the remarketing list itself are used as the source of an audience for a particular advertisement, a person's inclusion on such a list is nonetheless used to inform the automated bidding strategy that Google selects for an advertiser.

137. Google also uses data obtained via Google Ads and/or Analytics Source Code to inform its "Placements" advertising, which help an advertiser "determine the exact URLs" where their ads appear.[62] Advertisers can specify URLs within Google's Display Network (including

[58] *Data Sharing Settings*, ANALYTICS HELP, at *Details and benefits of each data sharing setting*, https://support.google.com/analytics/answer/1011397?hl=en#details-and-benefits&zippy=%2Cin-this-article.30%2Cin-this-article.

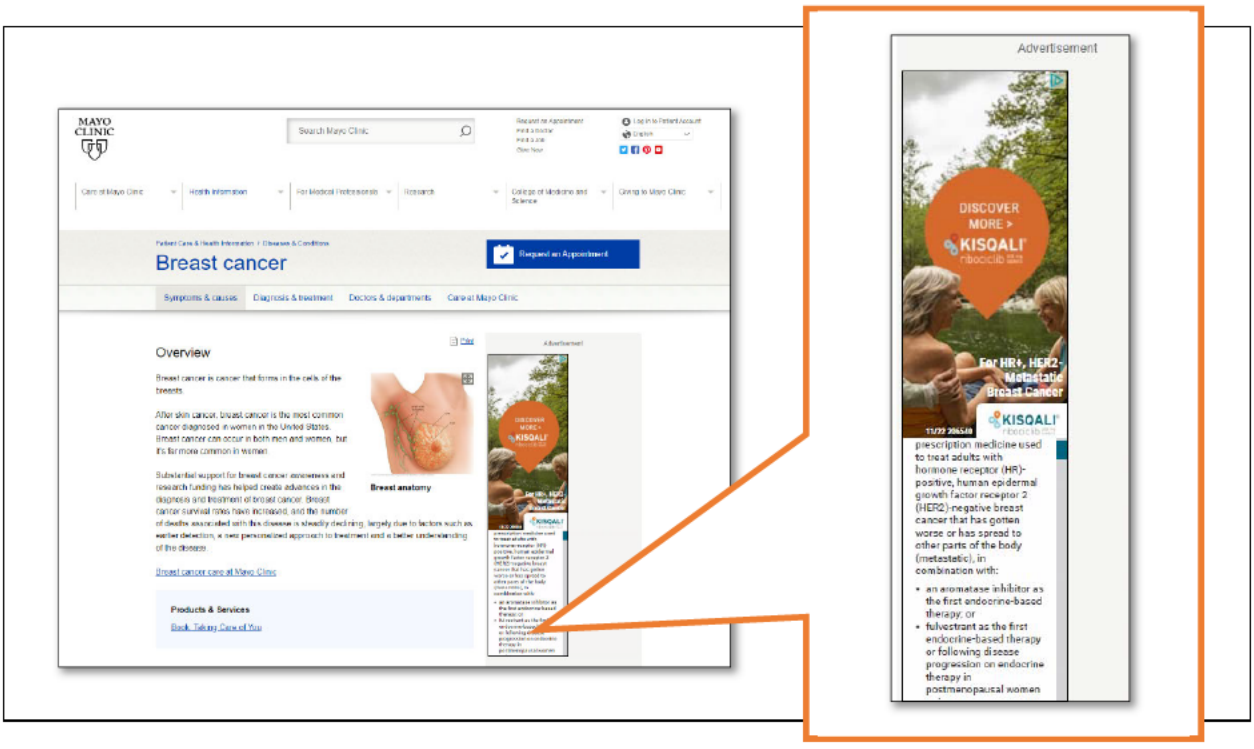
[59] *Id.*

[60] For avoidance of doubt, this action pertains to Google's tracking, acquisition, and its internal use of Health Information. It does not pertain to the sharing or sale of information to third parties through Google's Real-Time Bidding system. The Google Real-Time bidding system is the subject of an unrelated suit: *In re Google RTB Consumer Privacy Litig.*, Case No. 21-cv-02155-YGR-VKD (N.D. Cal.) (currently pending).

[61] *About Smart Bidding*, GOOGLE ADS HELP, https://support.google.com/google-ads/answer/7065882.

[62] About placement targeting, GOOGLE ADS HELP, https://support.google.com/google-ads/answer/2470108.

many Health Care Provider web properties) where they want their ads to appear, or they can allow Google to select the placements best suited to accomplish their goals, based upon Google's own "sorting" of candidate web properties, which in turn is based, in part, on "the past web traffic Google noticed on the site."[63] In the example below, a pharmaceutical company has placed an ad on the Mayo Clinic "Breast Cancer" page for its "Kisquali" drug to treat "Metastatic Breast Cancer."



138. On information and belief, the "past web traffic Google noticed," and uses to select placements on Health Care Provider web properties for advertisers, includes the activities of patients on Health Care Provider web properties, including on particularly sensitive pages like the above. In other words, Google uses its other (non-"ad") profiles of users based on Health Information (e.g. individuals with an interest in breast cancer) to assess which *websites* such individuals are likely to visit, and suggests advertisers target the website that Google "sorted" to the top based on the information. Google calls this "contextual," rather than "targeted" advertising, but it still leverages the Health Information intercepted from past visitors to target ads.

[63] *Id.*

139. Google also sells the option to run advertising campaigns guided by Google's artificial intelligence systems, such as "Performance Max." Google developed and uses its AI "to make more accurate predictions about which ads, audiences, and creative combinations perform best" for a particular advertiser. With information regarding the goals of a particular advertiser, "Google AI will then find potential customers for your goals and serve the most appropriate ad" across all of Google's advertising channels.[64] According to Google, Performance Max uses "Google's real-time understanding of user intent, behavior and context" to accomplish this. On information and belief, Google has used, and continues to use, the Health Information it obtained via both Google Ads source code and Google Analytics to develop, maintain, and improve its AI models for advertising, irrespective of any policy that may apply or be enforced with respect to a Health Care Provider's use of the information for its own advertising.

140. "Measur[ing] the effectiveness of advertising" is another way Google admits it uses Health Information, irrespective of any purported restrictions on personalized "ads." Google uses data obtained via Google Ads and/or Analytics Source Code for "Conversion Tracking" wherein Google monitors "what happens after a customer interacts with your ads," to help advertisers "[u]nderstand your return on investment (ROI) and make better informed decisions about your ad spend . . ., and [f]ind out how many customers may be interacting with your ads on one device or browser and converting on another," among other metrics.[65] Whether or not Google uses the information from intercepted communications with Health Care Providers, or the classifications it creates from that data to target a particular advertisement on that basis alone (as in "remarketing" uses), Google uses the data obtained from Health Care Provider websites to monitor which webpages on a Health Care Provider web property are most likely to result in clicks on viewed advertisements (to help advertisers make better informed decisions); and by monitoring the patient's activity, including activity on the Health Care Provider website, for purposes of

[64] *About Performance Max campaigns*, GOOGLE ADS HELP, https://support.google.com/google-ads/answer/10724817.

[65] *About conversion tracking*, GOOGLE ADS HELP, https://support.google.com/google-ads/answer/1722022.

identifying whether they take the action that the advertiser seeks to track. In the above "Placements" example on the Mayo Clinic web property, when such ads are presented on a Health Care Provider website, Google records that information via Google Ads Source Code to its systems so that it can track when and where the ad was shown. If the visitor clicks on the ad, Google records that information via Google Ads Source Code to its systems and monitors the visitor's later activity to determine whether they ultimately took the action identified as a "conversion" by the advertiser. "Attribution uses GA [Analytics], DCM [Doubleclick] and GDN [Display Network/Ads] logs as its primary data sources."[66] Such "attribution" of particular actions to advertisements is a significant part of Google's business.

141. Based on the fact that Plaintiffs' Health Care Provider web properties integrated Google Ads Source Code, the fact that Google does not purport to have any policy against measuring "the success of advertising" using Health Information, and Google's goals with respect to Google Analytics discussed in Section V(F), *infra*, Google used Plaintiffs' Health Information for advertising and Google's advertising machinery through, at a minimum, the methods described above.

b. Google Uses Health Information to Develop New Products and Services, Including Health Services

142. Developing, maintaining, and improving Google's Performance Max advertising AI and other advertising services, including systems to measure the effectiveness of ads, are far from the only Google business interests served by Plaintiffs' and Class members' Health Information. As Google reports in its Annual Form 10-K for the fiscal year ending December 31, 2022, filed with the Securities and Exchange Commission, "We face intense competition. If we do not continue to innovate and provide products and services that are useful to users, customers, and other partners, we may not remain competitive, which could harm our business, financial condition, and operating results."[67] Because Google does not even claim to exclude Health

[66] Ex. 10, *2017 Strategy Paper: Measurement*, GOOGLE (filed Aug. 6, 2024 in *United States v. Google LLC*, No. 1:23-cv-00108-LMB-JFA (E.D. Va. 2023), Dkt. 1132-2), at 76

[67] ALPHABET, INC., Annual Report (Form 10-K) (Dec. 31, 2022), https://abc.xyz/investor/static/pdf/20230203_alphabet_10K.pdf.

Information from being used in "develop[ing] new services," on information and belief, Google uses Plaintiffs' and Class members' Health Information to inform and develop new services. Indeed, Google's Form 10-K states that Google is "investing significantly in the areas of health, life sciences, and transportation, among others," and "[r]evenues from Other Bets [sources other than Google Services and Google Cloud] are generated primarily from the sale of health technology and internet services. [68]

c. Google Uses Health Information to Personalize "Content"

143. As noted above, Google claims to have policies restricting personalized "ads," but admits (while distracting with an overwhelming focus on "ads") that it personalizes "content" separate and apart from any such restrictions. As pertains to Health Information, Google does not even claim to prohibit itself from using its classifications of individuals who visit websites in categories such as "/Health/Aging & Geriatrics/Alzheimer's Disease." Google does not claim to prohibit itself from using its knowledge that a particular person uses a particular Health Care Provider and communications it intercepts about their health, to inform any and all aspects of what is presented on Google's products, other than perhaps (insofar as a policy is applied and enforced) by helping its customers serve an advertisement targeted specifically based on that information. Google thus purports to retain, and on information and belief, exercises, its self-anointed right, to "personalize" Google search results, recommendations on Google Maps, recommended apps on the Google Play Store, and other interactions with Google products, to patients based on their interactions with Health Care Providers and the inferences Google makes from the data it intercepts.

144. As Google explains on a deeply buried webpage about "Recommendation Systems" and machine learning: "How does YouTube know what video you might want to watch next? How does the Google Play Store pick an app just for you? Magic? No, in both cases, an ML-based [machine learning-based] recommendation model determines how similar videos and apps are to

[68] *Id.*

other things you like and then serves up a recommendation. . . . Homepage recommendations are personalized to a user based on their known interests. Every user sees different recommendations."[69] Recommendations and similar tailored content based upon Google's profiles for consumers are personalized advertisements by another name, differing only in that the primary, and often sole, "advertiser" and beneficiary in the case of each recommendation is Google. This webpage, for example, notes that "40% of app installs on Google Play come from recommendations," and "60% of watch time on YouTube comes from recommendations."[70]

F. At all Relevant Times, Google Acted with Full Knowledge and Intent

145. The transmission of volumes of Health Information to Google, demonstrated above, was no accident. Google intentionally marketed its tracking technologies in the healthcare industry. That marketing was extremely successful because, until circumstances forced it to reverse course, Google kept quiet about the fact that personally identifiable protected health information would invariably be transmitted through its products back to Google. Google knew exactly what would be transmitted to its servers as the developer of Google Source Code, and knew what was actually transmitted because it received and processed the data. Google at all relevant times acted with the intent to achieve the results that it did: extensive integration within Health Care Provider web properties across the United States, sending tens of millions of U.S. patients' identifiable sensitive information for Google's self-serving, and exceptionally profitable, use.

1. Google Intended for Its Third-Party Tracking Technology to Transmit the Communications and Activities Of Patients

146. Google intentionally marketed its third-party tracking technologies to Health Care Providers for the purpose of obtaining identifiable information relating to the health of patients, and deriving revenues from the information. A 2017 "Charter" document for Google Analytics (unsealed in other litigation on or around August 6, 2024) confirms that, no later than 2017, Google

[69] *Recommendations: what and why?*, GOOGLE MACHINE LEARNING, https://developers.google.com/machine-learning/recommendation/overview.

[70] *Id.*

specifically "[t]argeted" the "Healthcare" industry for Google Analytics, and that its "objective" in doing so was "to grow coverage of the overall media measurement of [Healthcare and other customers in particularly valuable "verticals"], and secondarily to drive new direct revenue for Google."[71]

147. Google's Analytics marketing adhered to its Charter. In Google's terminology, Health Care Providers and other advertisers are Google's customers, and the individuals who use their services are the advertiser's customers. For Health Care Providers, the customers are patients. Individuals who visit patients in the hospital, seek to apply for a job, or contact a Health Care Provider for research purposes are not the Health Care Provider's "customers." Google markets its Ads service as helping Google's customers "target your ads to the type of customers you want, and filter out those you don't."[72] Google markets its Analytics service as helping them "[g]et essential customer insights. Get a complete understanding of your customers across devices and platforms . . . and [u]ncover new insights and anticipate future customer actions."[73] When Google intentionally targeted the healthcare industry with this marketing, Google expressly invited Health Care Providers to track the communications and activities of their patients.

148. Indeed, as Google knew, only a limited subset of web pages on a Health Care Provider web property—pages unrelated to health, conditions, or payment—could reasonably be expected *not* to transmit Health Information where third-party tracking technology is present. This is clear in applicable laws such as HIPAA. The HHS Guidance discussed above makes it even more explicit. For Health Care Providers to track information and insights regarding only *non*-customers (non-patients) would be fundamentally at odds with the advertised benefits of these products. For Google to learn only about the communications and activities of non-patients from

[71] Ex. 11, *2017 Charter: Google Analytics*, GOOGLE, (filed Aug. 6, 2024 in *United States v. Google LLC*, No. 1:23-cv-00108-LMB-JFA (E.D. Va. 2023), Dkt. 1132-2), at 264.

[72] *Grow your business with Google Ads*, GOOGLE ADS HELP, https://support.google.com/google-ads/answer/6336021.

[73] *Analytics*, GOOGLE MARKETING PLATFORM, https://marketingplatform.google.com/about/analytics/.

its Health Care Provider customers would be inconsistent with the Google Analytics mission, reflected in its 2017 Charter, to be "the source of truth for understanding & taking action on a business' *customer* experience, behavior, and interactions."[74]

149. Google understood that Health Care Providers would use competitors' products, rather than Google's, unless Google's products were "useful" to them, [75] and thus did want or expect Health Care Providers to deploy Google Ads and Analytics technologies in large numbers solely for the minimally useful purpose of tracking non-patients and researchers. Google's objective was to "grow coverage of the overall media measurement" in "Health*care*," not health *research*.[76] Indeed, discouraging Health Care Providers from using Google Ads and Analytics products except in compliance with HIPAA (to track individuals other than their "customers"/patients only on pages unrelated to their primary business) would undermine, if not eliminate, Google's value proposition for the services.

150. Google's marketing succeeded. As of 2023, Google Ads and Google Analytics Source Code was exceptionally prevalent and widespread on Health Care Provider web properties, being used to track patients, and share Health Information, as Google intended.

2. Google Knew that It Would Intercept and Collect Health Information but Downplayed and Obscured that Reality to Expand its Reach in the Healthcare Industry

151. Google met its marketing objectives with respect to the healthcare industry by obscuring and minimizing the fact, known to Google as creator of the Google Source Code, that the Health Care Providers it targeted could not use Google's tools as advertised without Google's interception and collection of personally identifiable communications with patients. Google knew and must have known this would result in its receipt of Health Information.

152. Until in or around March 2023, as Google successfully expanded its access to patient data and providers across the health industry without attention from regulators or the public,

[74] Ex. 11, *2017 Charter: Google Analytics*, at 263 (emphasis added).

[75] *Annual Report (Form 10-K)*, ALPHABET, INC., at 10 (Dec. 31, 2022), https://abc.xyz/investor/static/pdf/20230203_alphabet_10K.pdf.

[76] Ex. 11, *2017 Charter: Google Analytics*, at 264.

its representations regarding Google Ads and Analytics hid Google's knowledge that it would, and did, obtain Health Information when Health Care Providers used the products. Google's disclosures with respect to Health Information intercepted by its third-party tracking technologies were limited to a "HIPAA disclaimer" at the bottom of a help page titled "Best practices to avoid sending Personally Identifiable Information (PII)," which stated:

> Unless otherwise specified in writing by Google, Google does not intend uses of Google Analytics to create obligations under the Health Insurance Portability and Accountability Act, as amended, ("HIPAA"), and makes no representations that Google Analytics satisfies HIPAA requirements. If you are (or become) a Covered Entity or Business Associate under HIPAA, you may not use Google Analytics for any purpose or in any manner involving Protected Health Information.[77]

153. Google did not enforce its admonition that covered entities "may not use" Google Analytics in a manner involving Protected Health Information. On the contrary, at all times while the Disclaimer was present at the end of Google's help page, Google marketed its third-party tracking technologies to the healthcare industry, with the outcome that, by 2023, it was present on several thousand covered entities' websites, sending protected health information to Google, as illustrated above. Google also implemented no features that would prevent Health Care Providers from implementing its tracking technology or prevent itself intercepting data from Health Care Providers' web properties, despite its self-serving Disclaimer.

154. Once a Health Care Provider installs Google Source Code on its web property, as 91% of those analyzed in Plaintiffs' pre-filing investigation have done, Google does not want them to remove it, does not want to exclude the data it receives from generating its own personalized

[77] *Best practices to avoid sending Personally Identifiable Information (PII)*, GOOGLE ANALYTICS HELP (archived March 5, 2023), https://web.archive.org/web/20230210102428/https://support.google.com/analytics/answer/6366371#zippy=%2Cin-this-article. Google does not offer Business Associate Agreements for its website tracking technologies because there is no way for those services to be useful to Health Care Providers, or Google, without collecting "individually identifiable health information" in violation of HIPAA and for Google's self-serving uses that are incompatible with HIPAA's protections. Google's technologies stand in stark contrast to other companies' services, which can be appropriate on a Health Care Provider web property, which do offer Business Associate Agreements, such as those offered by New Relic, Tealium, Microsoft, Adobe, and Amazon.

"content," and does not want them or stop using it for paid advertising. Google explains in its 2022 Form 10-K, "We generate a significant portion of our revenues from advertising. Reduced spending by advertisers, a loss of partners, or new and existing technologies that block ads online and/or affect our ability to customize ads could harm our business."[78]

155. Google's marketing, reflected in Google's 2019, 2021, and 2023 Google Analytics Terms of Service and various help pages associated with the services, therefore, downplayed and obscured the risks, realized in practice as Google Ads and Analytics Source Code proliferated, that any Health Care Provider using these products for their intended purpose of tracking "customers," (patients) would result in Google acquiring large volumes of identifiable private health information.

156. The Google Analytics Terms of Service do not expressly reference HIPAA, any other specific protection for Health Information, or the HIPAA Disclaimer on Google's help page. Instead, all versions of the contract misleadingly indicate that Google Analytics is automatically configured to **not** collect personally identifiable information at all, unless certain optional features are activated. Under the heading "Privacy," the 2019 and 2021 versions of the contract provided that "You will not and will not assist or permit any third party to, pass information to Google that Google could use or recognize as personally identifiable information."[79] In the context of other provisions in the documents, which identify what publishers "may not" and "must not" do, this representation about what "will not" occur reads like a promise that such transmissions can never happen. Even interpreted (favorably to Google) as a prohibition on Health Care Providers against sending identifiable data via Google Ads and Analytics services, the provision suggests that tracking on HIPAA-covered webpages *could* be anonymous, thus preserving patient confidentiality, and indeed, that such a configuration was the default.

[78] ALPHABET, INC., Annual Report (Form 10-K), at 9 (Dec. 31, 2022), https://abc.xyz/investor/static/pdf/20230203_alphabet_10K.pdf.

[79] Google amended the provision in May 2023 to include exceptions permitting the transmission of identifiable information to Google if they are consistent with other policies.

157. Google reinforced that impression on the same page where, until March 2023, it posted its HIPAA Disclaimer. The Disclaimer appeared at the bottom of a document titled "Best practices to avoid sending Personally Identifiable Information (PII)," which commenced with the assurance that, "To protect user privacy, Google policies mandate that no data be passed to Google that Google could use or recognize as personally identifiable information (PII)."[80] Further down in the document, but still well above the "HIPPA Disclaimer" at the bottom of the page, Google emphasized, *not* that Google Analytics is automatically and unavoidably designed to transmit identifiable data; *not* that linking Google Analytics to Google Ads renders "settings" to control how that identifiable data is used ineffective; and *not* that Google's marketing for Analytics as a tool to track "customers" necessarily means tracking patients' Health Information, but rather to a more mundane type of PII disclosure that Google's customers could actually control. Google highlighted that PII may be contained within the text of URLs and page titles, and should be removed from those:

> The basic Analytics tag collects the page URL and page title of each page that is viewed. PII is often inadvertently sent in these URLs and titles. Both the URL path and parameters must be free of PII. If there is any possibility of your URLs, URL parameters, or titles containing PII, you'll need to remove it.[81]

158. Google makes similar assurances, suggesting that identifiability is within Google's customers' control, regarding its other ads and marketing products. For Google Ad Manager, Google tells all publishers in its "Ad Manager and Ad Exchange program policies," that:

> In the interests of protecting user privacy, Google ads product policies mandate that publishers must not pass any data to Google that Google could use or recognize as personally identifiable information (PII).[82]

---

[80] *Best practices to avoid sending Personally Identifiable Information (PII)*, GOOGLE ANALYTICS HELP (archived March 5, 2023), https://web.archive.org/web/20230210102428/https://support.google.com/analytics/answer/6366371#zippy=%2Cin-this-article.

[81] *Id.*

[82] *Best Practices to Avoid Sending Personally Identifiable Information (PII)*, GOOGLE AD MANAGER HELP, https://support.google.com/admanager/answer/6156630.

In a related statement titled "False Positive and Personally Identifiable Information," Google tells publishers who have received a notification that they are sending PII what to do to either "fix the issue" or to identify whether there's a "common false positive" situation.[83]

159. Google furthers the impression that it does not collect personally identifiable information through its marketing of an "IP address masking" feature in Analytics. An older version of Google Analytics (which was used by many of the Health Care Providers analyzed by Plaintiffs) provides a setting that "truncates" the IP address of a person "as soon as technically feasible" by removing the "last octet of IPv4 user IP addresses and the last 80 bits of IPv6" after they are "sent to Google Analytics and asserting that "[t]he full IP address is never written to disk" when the feature is turned on.[84] Beginning in or around December 2022, Google began transitioning all publishers to "Google Analytics 4," where it states that "IP masking is not necessary since IP addresses are not logged or stored."[85] However, contrary to the impression that Google sought to provide in its marketing materials, Google Ads and Analytics products collect personally identifiable information by default, even if "fuzzified" by removing the last octet, as discussed above. Thus, the existence of the "IP address masking" feature itself is misleading because "masking" the IP address does not actually render the data anonymous.

160. In context, given the placement of the HIPAA Disclaimer, Google's choice not to expressly reference the Disclaimer in its form contracts, and the other assurances made above the Disclaimer and elsewhere, reasonable persons interpreting Google's representations regarding its Ads and Analytics products before May 15, 2023 could—and as evidenced by the 2017 Charter, were intended by Google to—conclude that Health Care Providers could use Google's third-party tracking technologies without even risking that Google would intercept identifiable data unless

[83] *False Positives and Personally Identifiable Information (PII)*, GOOGLE AD MANAGER HELP, at 1, https://support.google.com/admanager/answer/6157752.
[84] *IP masking in Universal Analytics*, GOOGLE ANALYTICS HELP, https://support.google.com/analytics/answer/2763052.

[85] *Id.* As of July 1, 2023, Google announced that "new data will only flow into Google Analytics 4 properties" after that date. *Introducing the next generation of Analytics*, GOOGLE ANALYTICS HELP, https://support.google.com/analytics/answer/10089681.

they affirmatively chose to and/or mistakenly transmitted it in the text of a URL. Google's HIPAA Disclaimer reasonably looked like nothing more than a precaution by Google against an unlikely but theoretically possible occurrence, not a meaningful warning that, for Health Care Providers, identifiable transmissions of Health Information would be all but guaranteed.

161. That Google intended to gain access to Health Information, and that—whatever Health Care Providers consented to in the Google Analytics Terms of Service, it was not to include Google in communications relating to their patients' health, or to disclose any Health Information to Google—is also evident in the fact that Google's efforts were successful. Google intercepted the communications and obtained the information. As Health Care Providers come to understand this, they are issuing breach notifications, expressing that they did not know that would occur. [86]

3. Google's March 2023 Admonition About Transmitting Health Information Is Farcical

162. In or around March 2023, several months after HHS issued its Guidance in response to evidence concerning Google's third-party tracking technology, Google removed the Disclaimer from the help page where it appeared, and posted a new "help" page for Google Analytics titled, "HIPAA and Google Analytics," which acknowledges the now widely understood reality that Google Analytics on Health Care Provider web properties is (consistent with the purposes of Google Analytics tools, to track "customers," *i.e.* patients) a HIPAA violation.[87]

[86] *See* Ex. 12, *Advocate Aurora Health Data Breach Affects 3 Million Patients*, AAPC (October 27, 2022), https://www.aapc.com/blog/86572-advocate-aurora-health-data-breach-affects-3-million-patients ("We recently learned that, in certain circumstances, [website tracking technologies] transmitted certain patient information to third-party analytics vendors . . . particularly for users concurrently logged into their Facebook or Google accounts."); Ex. 13, *Notice of data privacy incident from Allina Health*, ALLINA HEALTH (April 28, 2023), https://www.allinahealth.org/about-us/news-releases/2023/notice-of-data-privacy-incident-from-allina-health ("In recent months, several health care systems have learned that the tools used by internet tracking technology providers may inadvertently capture private health information."); Ex. 3, (Kaiser, *supra*) ("On October 25, 2023, Kaiser Permanente determined that [website tracking technologies] may have transmitted personal information to . . . Google").

[87] *HIPAA and Google Analytics*, Google Analytics Help https://support.google.com/analytics/answer/13297105.

163. Google's own generative AI product, Google Bard, has also acknowledged that Google's tracking technologies are not appropriate in this context:

164. Yet Google still collects Health Information through the same methods today as it did prior to posting its warning in March 2023. Even after March 2023, Google's "HIPAA and Google Analytics" help page does not reflect any intent to deter Health Care Providers from using and continuing to use its products for their advertised purposes, which many are doing, but rather reflects Google's recognition that Google could face liability for its conduct in obtaining Health Information as alleged herein, and was intended to provide a modicum of deniability. On information and belief, Google has not posted any such admonitions specific to other Google Ads services.

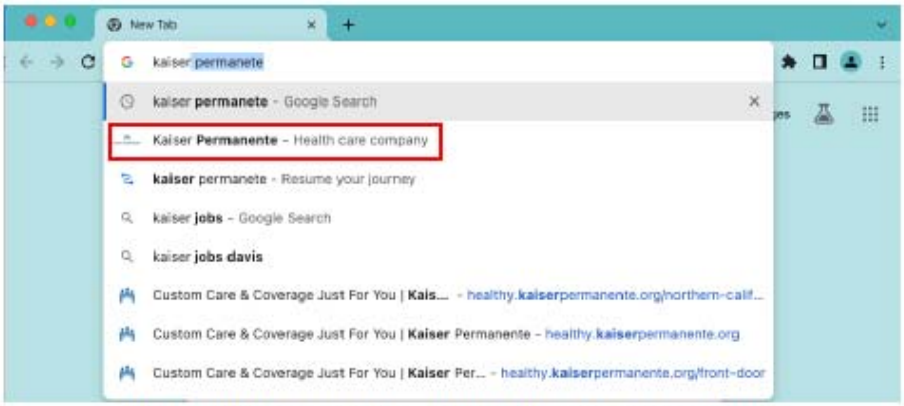
165. Given the purposes for which Google markets Google Ads and Google Analytics products, *i.e.*, to track and obtain insights about an advertiser's "customers," any claim that Google believed its products were exceptionally popular with Health Care Providers solely for tracking and advertising activities unrelated to their primary business—the provision of healthcare to patients—would have been irrational.

166. Any such belief or expectation was also irrational with reference to the information available to Google. Google receives each transmission from each Health Care Provider web property where Google Source Code operates and thus has all information required to know and understand when the transmissions contain Health Information and the contents of patient communications. At all relevant times, Google knew and knows: (i) when the source of the

transmission is a Health Care Provider web property; (ii) when the contents of the transmission are identifying; and (iii) when the contents relate to the physical or mental health, conditions, the provision of healthcare, or payment, i.e., are Health Information.

a. Google Knows When Health Care Providers Transmit Information to It

167. Google knows when the source of each transmission is a Health Care Provider web property because each transmission contains the URL of the web property. While the source of a transmission would be obvious or at least readily determined by anyone from the URL itself, it is especially clear to Google, because Google maintains a "search index" built through the work of software known as crawlers [that] automatically visit publicly accessible webpages and follow links on those pages. The Index "contains hundreds of billions of webpages and is well over 100,000,000 gigabytes in size."[88] For each webpage, Google has already conducted an "indexing" process that "includes processing and analyzing the textual content and key content tags and attributes, such as <title> elements and alt attributes, images, videos, and more," to determine what the page is about.[89] In the Google Chrome browser, for example, based on Google's pre-existing analysis of web properties, Google automatically categorizes web-properties including the Health Care Provider web properties Plaintiffs visited as belonging to a "Health care company":

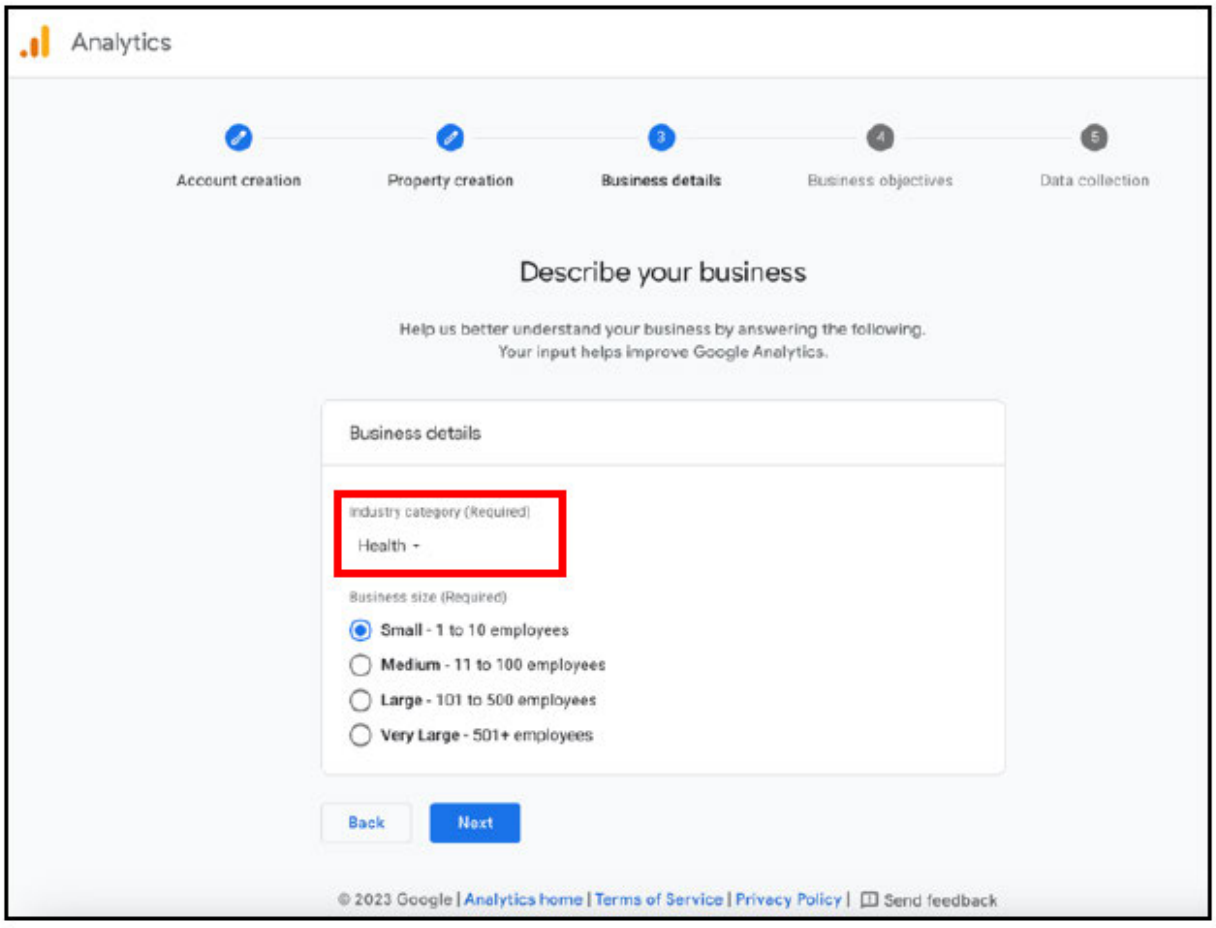


Kaiser Permanente – "Health care company"

[88] *Organizing Information - How Google Search Works*, GOOGLE SEARCH, https://www.google.com/search/howsearchworks/how-search-works/organizing-information.

[89] *Id.*

168. In addition, each entity using Google Ads and Google Analytics services must register for an account to use the services, and in (at least) the case of Analytics, is required to identify their "industry category," for which one of the drop-down menu options is "Health." Based upon the results of counsel's investigation, it is likely that over 3,000 entities (60% of 5,297 Health Care Providers using Google Analytics) affirmatively reported their industry as "Health" during the sign-up process.



169. In addition, the information transmitted to one or more Google domains on webpages where Google Source Code is present invariably contains at least one value that reflects the identity of the entity transmitting the information. Below is an index explaining the values

typically transmitted by one or more of the Google Source Code systems on Plaintiffs' Health Care Providers' web properties with a brief description of their meaning.

Field	Value and Explanation
tid	Explanation: Google explains that the "tid" equals an alphanumeric value that is a "tracking ID/web property ID. The format [of the value] is UA-XXXX-Y. All collected data is associated by this ID."[90]
gtm	Explanation: This field equals an alphanumeric value that corresponds to the advertiser's Google Tag Manager account.[91] It can therefore identify the patient's Health Care Provider (e.g. where the proposed targeted advertisement may appear).

b. Google Knows the Transmissions it Receives are Identifiable.

170. Google knows when the contents of each transmission are identifiable with respect to the individual whose actions are being tracked because they invariably are. Google designed its source code to send Identifiers with the transmissions, and as a result each transmission in fact contains one or more Identifiers readable in Google's systems. Google made special efforts to ensure that website visitors, *i.e.* Plaintiffs and Class Members themselves, could not prevent identifiable information from being transmitted to Google with the other contents of their Health Information. The Google cookies are designed to avoid any attempts by Plaintiffs and Class Members to block transmissions to Google. In designing Google's cookies as disguised first-party cookies, Google was aware that its technology would circumvent browser-based efforts to block third-party cookies and related privacy settings.

c. Google Knows When the Identifiable Transmissions Relate to Healthcare

171. Google knows when the contents of each transmission do, and do not, contain Health Information because Google receives the contents of each transmission. Google maintains an extensive infrastructure for processing and analyzing such contents to determine their meaning. Google in fact categorizes the contents of each transmission using verticals or a similar taxonomy

[90] Ex. 8, *Measurement Protocol Parameter Reference,* at 1.

[91] *Set Up and Install Tag Manager*, GOOGLE TAG MANAGER HELP, at 2, https://web.archive.org/web/20240208093148/https://support.google.com/tagmanager/answer/6103696.

which includes values for categorizations pertaining to mental or physical health and conditions, at a minimum. Upon confirming that transmissions contain Health Information, Google does not enforce any policy prohibiting the transmission of such information. Google does not notify Health Care Providers when they send information to Google in violation of HIPAA. Absent such a notification, Google does not share with Health Care Providers any information concerning the specific webpages that do, or do not, contain information relating to patients' health. To the extent Google claims to take any action to protect privacy in such information at all, Google only claims to exclude the information from being used in some, not all, of Google's advertising products and services. Google takes no action to exclude the information from being used in Google's other services, to improve those services, or to develop new ones.

172. That Google knows, understands, and intends to engage in the conduct alleged is further evidenced by the following facts: Google's conduct (i) has been a subject of national news and breach notifications by Health Care Providers; (ii) resulted in multiple updates and amendments to HHS Guidance in response to Google-specific evidence; and (iii) resulted in this litigation, wherein Plaintiffs provided Google with a list of all Health Care Provider websites which Plaintiffs' experts identified transmissions via Google Source Code on or around July 2023.

173. Despite plain, and mounting, evidence that Google receives Health Information via Google Source Code, on information and belief, as of this filing Google still does not enforce any policy prohibiting such transmissions and is still intercepting Health Information.

G. Plaintiffs and Class Members Reasonably Do Not Expect Google's Conduct and Did Not Consent

174. Each Plaintiff expected that Google would not obtain, analyze, or use the Health Information they exchanged with their respective Health Care Providers, and would not be privy to the contents of their electronic communications with Health Care Providers. Each Plaintiff's expectation was reasonable for several reasons.

175. The confidentiality, sensitivity and inherent privacy of Health Information have been recognized and held firm throughout history and within current legal frameworks. Indeed,

the confidentiality of Health Information finds its origins as far back as 400 B.C., in the original Hippocratic Oath:

> Whatever I see or hear in the lives of my patients, whether in connection with my professional practice or not, which ought not to be spoken of outside, I will keep secret, as considering all such things to be private.[92]

176. That Oath is embodied today in the legal concept of a medical provider's duty of confidentiality. *See, e.g.*, American Medical Association's ("AMA") Code of Medical Ethics Opinion 3.1.1. (affirming that "protecting information gathered in association with the care of the patient is a core value in health care" and "[p]atient privacy encompasses a number of aspects including…personal data (informational privacy . . .)" . . ."Physicians must seek to protect patient privacy in all settings to the greatest extent possible…");[93] AMA Code of Medical Ethics Opinion 3.2.4 (confirming expectation of privacy over health-related information and stating that third-party access for commercial purposes can only occur if information has been de-identified and with full disclosure to patients); [94] AMA Code of Medical Ethics Opinion 3.3.2 (same).[95]

177. Health Care Providers are governed by HIPAA which, as set forth above, prohibits disclosure of "individually identifiable health information," including through Google's third-party tracking technology. Indeed, federal and state law grant patients the right to protect the confidentiality of data that identifies them as patients of a particular health care provider and restrict the use of their health data, including their status as a patient, to only uses related to their care or otherwise authorized by federal or state law in the absence of patient authorization.

---

[92] Michael North, *Translation of Original Hippocratic Oath*, NAT'L LIBR. OF MED., at 2, https://www.nlm.nih.gov/hmd/greek/greek_oath.html.

[93] *Privacy in Health Care: Code of Medical Ethics Opinion 3.1.1*, AM. MED. ASS'N, https://code-medical-ethics.ama-assn.org/sites/default/files/2022-08/3.1.1.pdf.

[94] *Access to Medical Records by Data Collection Companies: Opinion 3.2.4*, AM. MED. ASS'N, https://code-medical-ethics.ama-assn.org/sites/default/files/2022-08/3.2.4.pdf.

[95] *Confidentiality & Electronic Medical Records: Code of Medical Ethics Opinion 3.3.2*, AM. MED. ASS'N, https://code-medical-ethics.ama-assn.org/sites/default/files/2022-08/3.3.2.pdf.

178. Google is a California-based corporation and its Terms of Service expressly adopt California law,[96] which further protects Health Information by statute, including through the California Invasion of Privacy Act (CIPA), Confidentiality of Medical Information Act (CMIA), California Consumer Privacy Act (CCPA), and California Civ. Code § 1798.91.

179. Common law privacy torts, such as intrusion upon seclusion, public disclosure of private facts, and breach of fiduciary duty create and support a reasonable expectation that individuals' Health Information will not be shared or otherwise intercepted without their knowledge or authorization.

180. Common law rights against trespass to personal property create and support a reasonable expectation that individuals' browsers and devices will not be used to facilitate the transmission of their Health Information without their knowledge or authorization.

181. Google promises that Google does not collect Health Information that individuals do not choose to provide to Google. Under the sub-heading "Categories of information we collect," the Google Privacy Policy identifies "health information" as a distinct category of information, and explains that Google's collection of this information is limited to only when a person "choose[s] to provide it": "Health information *if you choose to provide it*, such as your medical history, vital signs and health metrics (like blood glucose levels), and other similar information related to your physical or mental health, in the course of using Google services that offer health-related features, such as the Google Health Studies app."[97]

182. Google promises that neither Google nor any "advertiser," including without limitation any Health Care Provider using Google Ads or Google Analytics, will "use topics or

[96] *See* Ex. 9, *Terms of Service*, (asserting that "California law will govern all disputes arising out of or relating to these terms, service-specific additional terms, or any related services, regardless of conflict of laws rules"). Because the most recent Terms of Service for United States users when Plaintiffs brought this action states that it is effective as of January 2022, citations to Google's Terms of Service herein are to the January 2022 version, which is attached as Exhibit 9.

[97] Ex. 14, *Privacy Policy*, Google Privacy & Terms (Dec. 15, 2022) at 17-18 (emphasis added). As noted above, Google has revised its policy seven times since this action was filed. The promise "health information, if you choose to provide it" appears in all versions.

show personalized ads" based on health. Under the heading "Why Google Collects Data," in Google's Privacy Policy, Google declares that Google does not show "personalized ads based on sensitive categories," such as . . . health, where the underlined text expands to declare: "We don't use topics or show personalized ads based on sensitive categories like race, religion, sexual orientation, or health. And we require the same from advertisers that use our services."[98] Google repeats and expands upon its promises on the webpage incorporated at the "require the same from advertisers" hyperlink, stating that it prohibits advertising based on: "Restricted drug terms," such as "prescription medications and information about prescription medications . . . .;" and "personal health content," such as "physical or mental health conditions, including diseases, sexual health, and chronic health conditions"; "[p]roducts, services, or procedures to treat or manage chronic health conditions…"; "any health issues associated with intimate body parts or functions…"; "invasive medical procedures"; and, "[d]isabilities, even when content is oriented toward the user's primary caretaker," and again confirms that "We don't allow targeting users based on legally restricted content."[99]

183. Google's violation of Plaintiffs' and Class members' reasonable expectations is highly offensive and would be considered highly offensive to a reasonable person. The extent of the intrusion cannot be fully known, as the nature of privacy invasion involves using Plaintiffs' and Class Members' Health Information for potentially countless unauthorized purposes, known and unknown, in perpetuity.

184. Google's deployment of third-party cookies disguised as first-party cookies that are placed on Plaintiffs' and Class Members' computing devices to effectuate its objectives for Google Analytics and other Google Source Code is highly offensive in itself, and even more so in the context of interactions with a Health Care Provider. Also supporting the highly offensive nature

[98] Ex. 14, *Privacy Policy*, at 5-6, 30 (underline/hyperlink original).

[99] Ex. 15, *Personalized Advertising*, GOOGLE ADVERTISING POLICIES HELP, https://support.google.com/adspolicy/answer/143465, at 4, 5, 8.

of Google's conduct is the fact that Google acted surreptitiously and with the goal of profiting from the data it obtained.

185. Google's actions have not only harmed Plaintiffs and Class members directly, they are also harming society. "The prospect of releasing highly sensitive [protected health information (PHI)] can result in medical mistrust and the deterioration of the confidential, safe environment that is necessary to quality health care, a functional health care system, and the public's health generally." "[A]n individual's lack of trust in their health care provider to maintain the confidentiality of the individual's most sensitive medical information and a lack of trust in the medical system more generally may have significant repercussions for the public's health more generally."[100]

H. Google's Conduct Benefits Google and Harms Class Members

186. By minimizing, in its Analytics Terms of Service and throughout its marketing materials including help pages, the risks that Google would obtain Health Information when Health Care Providers use Google's Ads and Analytics services—uses which Google knew and understood at all relevant times, but of which regulators and the public have only more recently become aware—Google successfully obtained at least several thousand customers for its Ads and Analytics services that it should not have obtained. Google benefited each time its Health Care Provider customers paid Google for advertising services (targeted or not), and each time its other advertising customers paid Google for advertising services that were developed, maintained, or improved with the use of Class members' Health Information, as well as for Placements and other purportedly non-targeted advertising that relied in whole or in part on that information.

187. Google also benefited from using the Health Information it received in other ways, including without limitation by using the Health Information for Google's advertising and other

[100] *See HIPAA Privacy Rule To Support Reproductive Health Care Privacy*, U.S. DEP'T OF HEALTH AND HUM. SERV. (Apr. 17, 2023), https://www.federalregister.gov/documents/2023/04/17/2023-07517/hipaa-privacy-rule-to-support-reproductive-health-care-privacy.

purposes described above, and by merely possessing Class members' Health Information as an asset. It is widely recognized that "Big data now represents a core economic asset that can create significant competitive advantage for firms and drive innovation and growth."[101] A 2019 study calculated the value of Americans' personal information gathered and used by Google to be $15.3 billion in 2016, $18.1 billion in 2017, and $21.5 billion in 2018.[102] While the exact value of Plaintiffs' and Class Members' Health Information in this action will be a matter for expert determination, it is clear that its value is substantial.

188. Plaintiffs and Class members, meanwhile, were harmed by the same conduct. Their privacy was violated.[103] Their browsers and devices were used by Google against their will, without their knowledge, and without their consent. They lost control over information that should not have been copied to Google's systems for any purpose other than those expressly authorized by HIPAA and the CMIA, and certainly not for uses in Google's advertising machinery and to further Google's other business interests. Plaintiffs and Class members do not know what

[101] *Supporting Investment in Knowledge Capital*, Growth and Innovation, OECD PUBLISHING 1, 319 (Oct. 13, 2013), https://www.oecd-ilibrary.org/industry-and-services/supporting-investment-in-knowledge-capital-growth-and-innovation_9789264193307-en; Alessandro Acquisti, Curtis Taylor, and & Liad Wagman, *The Economics of Privacy*, 54 J. OF ECON. LITERATURE 442, 444 (June 2016), https://www.heinz.cmu.edu/~acquisti/papers/AcquistiTaylorWagman-JEL-2016.pdf (noting "obvious and substantial economic value."); *The World's Most Valuable Resource is No Longer Oil, but Data*, THE ECONOMIST (May 6, 2017), https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data (comparing the digital market for user data to be analogous to the oil industry); SHOSHANA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM, 166 (2019) (explaining that revenue from user data pervades every economic transaction in the modern economy); Paul M. Schwartz, *Property, Privacy, and Personal Data*, 117 HARV. L. REV. 2055, 2056-57 (2004) ("[t]he monetary value of personal data is large and still growing….Companies view this information as a corporate asset and have invested heavily in software that facilitates the collection of consumer information").

[102] Robert Shapiro & Siddhartha Aneja, *Who Owns Americans' Personal Information and What Is It Worth?*, FUTURE MAJORITY, at 3 (March 2019), https://assets.futuremajority.org/uploads/report-for-future-majority-on-the-value-of-people-s-personal-data-shapiro-aneja-march-8-2019.pdf.

[103] Amnesty International, *Surveillance Giants: How the Business Model of Google and Facebook Threatens Human Rights*, AMNESTY INT'L 1, at 5-6 (Nov. 21, 2019), https://www.amnesty.org/en/documents/pol30/1404/2019/en/ (opining that Google and other companies engage in a "surveillance-based business model" that, among other things is "an assault on the right to privacy on an unprecedented scale").

"recommendations" they have received from Google based on their Health Information, or how Google "personalized" their interactions with Google services based on health-related topics that Google acknowledges are "sensitive." They do not know how else Google used their information, whether to inform its strategic entry into parts of the healthcare industry, or to train Artificial Intelligence to "chat" realistically with individuals suffering from particular conditions.

189. In addition, to the extent Plaintiffs may have wanted to grant access to their Health Information to Google or any entity other than their Health Care Provider, Google misappropriated the data and its value. There are market exchanges where individuals, like Plaintiffs and Class Members, can sell or monetize their own data. For example, Nielsen Data, Killi, DataCoup, AppOptix and Mobile Computer will pay users for their data.[104] Similarly, Google itself has launched programs that pay users for their data. This includes a program called Screenwise -- an opt-in panel that can be installed on the Chrome Browser and permit Google to track and record individuals' browsing history in exchange for payment.[105] Nielsen, UpVoice, HoneyGain, and SavvyConnect are all additional companies that pay for browsing history information. Because Americans typically do not want to sell their individually identifiable health information for any purpose and authorized recipients are prohibited from sharing or selling it on the market, there are fewer open markets for a license to collect or sell individually identifiable health information for non-health purposes than other types of data. However, black markets do exist for such data. It has been reported that health data can be "more expensive than stolen credit card numbers" on black markets.[106]

190. In addition, Google Account Holders, who entered into contractual agreements with Google, lost the benefit of their bargain when Google took more data than the parties agreed would

[104] *See e.g.*, Kevin Mercandante, *Ten Apps for Selling Your Data for Cash*, BEST WALLET HACKS (June 10, 2020), https://wallethacks.com/apps-for-selling-your-data/.

[105] Jack Marshall, *Google Pays Users for Browsing Data*, DIGIDAY (Feb. 10, 2012), https://digiday.com/media/google-pays-users-for-browsing-data/.

[106] Aarti Shahani, *The Black Market for Stolen Health Care Data*, NPR: ALL TECH CONSIDERED, at 3 (Feb. 13, 2015 4:55 AM ET), https://www.npr.org/sections/alltechconsidered/2015/02/13/385901377/the-black-market-for-stolen-health-care-data.

be exchanged, and used it for purposes for which the contract indicated it would not be used. Those benefit of the bargain damages also include, but are not limited to: (i) loss of the promised benefits of their Google Account Holder experience; (ii) out-of-pocket costs; (iii) loss of control over property which has marketable value; and (iv) Google obtained more compensation from the Plaintiffs (in the form of data) than it was entitled to obtain through its contract of adhesion

VI. CLASS ACTION ALLEGATIONS

191. Plaintiffs file this as a class action on behalf of themselves and the following class and subclass:[107]

> **ALL U.S. HEALTH USER CLASS** – All persons in the United States and its territories whose Health Information was obtained by Google through Google Source Code from their Health Care Provider.
>
> **GOOGLE ACCOUNT HOLDER SUBCLASS** – All Google Account Holders in the United States and its territories whose Health Information was obtained by Google through Google Source Code from their Health Care Provider.

192. Excluded from the Class are counsel for Plaintiffs, the Court and its personnel and immediate family members, and the Defendant and its officers, directors, employees, affiliates, legal representatives, predecessors, successors and assigns, and any entity in which any of them has a controlling interest.

193. The members of the Class and Subclass are so numerous that joinder is impracticable.

194. Common questions of law and fact are apt to drive resolution of the case, exist as to all members of the Class and Subclass, and predominate over any questions affecting solely individual members including, but not limited to, the following:

a. Whether Google unlawfully obtains Health Information from HIPAA-covered entities through Google Ads;

b. Whether Google unlawfully obtains Health Information from HIPAA-covered entities through Google Analytics;

[107] Plaintiffs reserve the right to modify the Class and Subclass Definition at the class certification stage or as otherwise instructed by the Court.

c. Whether Google uses Health Information for advertising purposes;

d. Whether Google uses Health Information for personalizing content and/or recommendations to users;

e. Whether Google uses Health Information to develop new products;

f. Whether Google uses Health Information to improve its products;

g. Whether Google uses Health Information to develop new businesses;

h. Whether the Google Terms of Service includes binding contractual promises;

i. Whether the webpages incorporated by reference in the Google Terms of Service include binding contractual promises;

j. Whether Google's tracking, collection and/or monetization of Health Information constitutes a breach of contract with Google Account Holders;

k. Whether Google's form policies and contract documents demonstrate consent from Class members to Google's acquisition of their Health Information through the Google Source Code;

l. Whether Google's form policies and contract documents demonstrate consent from Health Care Providers to Google's acquisition of Class members' Health Information through the Google Source Code;

m. Whether any consent from Health Care Providers to Google's acquisition of Class members' Health Information through the Google Source Code was obtained for a criminal or tortious purpose;

n. Whether Class Members have a reasonable expectation of privacy over their Health Information;

o. Whether Google's collection and/or use of Health Information constitutes highly offensive conduct;

p. Whether Google was unjustly enriched as a result of its violations of Plaintiffs' and Class Members' privacy rights;

q. Whether the Health Information at issue is "content" under the ECPA;

r. Whether the Health Information at issue has economic value; and

s. Whether Google unjustly profited from the conduct alleged herein.

195. Plaintiffs' claims are typical of the claims of other Class Members, as all members of the Classes were similarly affected by Google's wrongful conduct in violation of federal and California law, as complained of herein.

196. Plaintiffs will fairly and adequately protect the interests of the members of the Classes and have retained counsel that is competent and experienced in class action litigation. Plaintiffs have no interests that conflict with, or are otherwise antagonistic to, the interests of other Class Members.

197. A class action is superior to all other available methods for the fair and efficient adjudication of this controversy since joinder of all members is impracticable. Further, as the damages that individual Class Members have suffered may be relatively small, the expense and burden of individual litigation make it impossible for members of the Class as to individually redress the wrongs done to them. There will be no difficulty in management of this action as a class action.

VII. TOLLING

198. Any applicable statute of limitations has been tolled by Defendant's knowing and active concealment of the conduct and misrepresentations and omissions alleged herein. Through no fault or lack of diligence, Plaintiffs and members of the Classes were deceived and could not reasonably discover Defendant's deception and unlawful conduct.

199. Plaintiffs and members of the Classes did not discover and did not know of any facts that would have caused a reasonable person to suspect that Defendant was acting unlawfully and in the manner alleged herein. As alleged herein, the representations made by Google were material to Plaintiffs and members of the Classes at all relevant times. Within the time period of

any applicable statutes of limitations, Plaintiffs and members of the Classes could not have discovered through the exercise of reasonable diligence the alleged wrongful conduct.

200. Particularly in light of the sensitivity of Health Information as a category, privacy expectations rooted in federal and state law regarding such information, the invisibility of Google Source Code on affected web properties, at all times; Google's active and intentional deployment of the Google Source Code in the healthcare industry; Google's unique knowledge that it would and did obtain Health Information via Google Source Code on Health Care Provider web properties; and Google's activities to prevent Health Care Providers from understanding that reality for years, Google is and was under a continuous duty to disclose to Plaintiffs and members of the Classes the true nature of the disclosures being made and the lack of an actual "requirement" before the data was shared with it.

201. Defendant knowingly, actively, affirmatively and/or negligently concealed the facts alleged herein. Plaintiffs and members of the Classes reasonably relied on Defendant's concealment.

202. Further, Defendant's unlawful tracking, collection, and monetization of Plaintiffs and Class Members' Health Information was done surreptitiously in a manner undetectable by patients. As a result, despite Plaintiffs' and Class Members' exercise of due diligence, they could not, and did not, discover the unlawful conduct described herein.

203. Plaintiffs only became aware of Google's wrongdoing alleged herein shortly before the filing of this complaint as a result of counsel's investigation.

204. For these reasons, all applicable statutes of limitation have been tolled based on the discovery rule and Defendant's concealment, and Defendant is estopped from relying on any statutes of limitations in defense of this action.

VIII. CAUSES OF ACTION

COUNT ONE
VIOLATION OF THE ELECTRONIC COMMUNICATIONS PRIVACY ACT
(On Behalf of All Classes)

205. Plaintiffs hereby incorporate the factual allegations set forth above by reference.

206. The ECPA prohibits the intentional interception of the contents of any electronic communication. 18 U.S.C. § 2511.

207. Under the Act, an "electronic communication" is defined as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce."

208. The Plaintiffs' communications with Health Care Provider web-properties described herein are "electronic communications" under the Act.

209. Under the Act, "interception" is defined as the "acquisition of the contents of any … electronic communication … through the use of any … device."

210. The ECPA protects both the sending and receiving of communications and provides a private right of action to any person whose electronic communications are intercepted. *See* 18 U.S.C. § 2520(a).

211. Google intentionally intercepted, i.e., acquired, Plaintiffs' and Class Members' Health Information on their Health Care Providers' web properties where the Google Source Code was present. As set forth above, Google targeted the healthcare industry to implement Google tracking technologies, knowing the use of the technologies on Health Care Provider web properties would transmit Health Information from patient visitors.

212. Google's acquisition of Health Information was contemporaneous with their making.

213. The Act expressly states that communications' "contents … includes any information concerning the substance, purport, or meaning of that communication."

214. As alleged herein, the transmissions of Health Information between Plaintiffs and Class Members and their Health Care Providers qualify as "contents" of communications under the ECPA's definition. The intercepted communications contents include, but are not limited to:

a. the precise content of patient registrations, including information that Plaintiffs and patients input into online forms in the process of patient registration and communications exchanged during the registration to indicate patient status and sign-ups;

b. the precise content of patients' access to and communications with their Health Care Provider within authenticated patient portals, such as logging-in or logging out of a patient portal and exchanging communications about appointments, treatments, conditions, allergies, medical records, payments, or providers inside the portals;

c. the precise content of searches that patients conduct on Health Care Provider web properties for providers, treatments, conditions, payment information, insurance, and more; and

d. the precise content of patients' access to and communications with their Health Care Provider on pages directed towards patients outside of the patient portal, which includes communications relating to specific doctors, symptoms, conditions, treatments, prescription drugs, and requests for appointments.

215. The following constitute "devices" within the meaning of 18 U.S.C. § 2510(5):

a. The Google cookies used to track patients' communications;

b. Patients' browsers;

c. Patients' computing devices;

d. Google's web-servers;

e. The web-servers of Health Care Providers' web properties where the Google Source Code was present; and

f. The Google Source Code deployed by Google to effectuate its acquisition of patient communications.

216. Google is not a party to Plaintiffs' and Class Members' communications with their Health Care Providers.

217. Google intercepted and received Plaintiffs' and Class Members' Health Information through the surreptitious redirection from Plaintiffs' and Class Members' computing devices to Google via the Google Source Code.

218. Neither Google nor the Health Care Providers obtained Plaintiffs' and Class Members' lawful consent or authorization for Google's acquisition of Health Information.

219. Google did not require any Health Care Provider to obtain lawful rights to share Plaintiffs' and Class Members' Health Information with Google.

220. Any purported consent that Google received from Health Care Providers to obtain Plaintiffs' and Class Members' Health Information was and is not valid because HIPAA prohibits a Health Care Provider from disclosing patient Health Information without the patient's express written authorization (*see* 45 C.F.R. § 164.508(a)(3)) and a lack of patient authorization violates the FTC's Health Breach Notification Rule (16 C.F.R. § 318 *et seq*.).

221. Any purported consent that Google received from Health Care Providers to obtain Plaintiffs' and Class Members' Health Information was and is not valid because Google obscured and misrepresented the nature of its tracking tools to Health Care Providers. As set forth above in Section V(F), Google made false assurances to Health Care Providers that Google does not obtain personally identifiable information via its tracking tools and/or that certain settings of the tracking technologies (e.g., IP masking) can prevent the transmission of Health Information to Google.

222. In acquiring Plaintiffs' and Class Members' Health Information, Google had a purpose that was tortious, criminal, and designed to violate constitutional and statutory provisions including, but not limited to:

a. The unauthorized acquisition of individually identifiable health information is tortious in and of itself regardless of whether the means deployed to acquire the

information violates the Wiretap act or any subsequent purpose or use for the acquisition. Google intentionally committed a tortious act by acquiring individually identifiable health information without authorization to do so;

b. The unauthorized acquisition of individually identifiable health information is a criminal violation of 42 U.S.C. § 1320d-6 regardless of any subsequent purpose or use of the individually identifiable health information. Google intentionally violated 42 U.S.C. § 1320d-6 by intentionally acquiring individually identifiable health information without authorization;

c. A violation of HIPAA, particularly 42 U.S.C. § 1320d-6, which is a criminal offense punishable by fine or imprisonment with increased penalties where "the offense is committed with intent to sell, transfer, or use individually identifiable health information for commercial advantage [or] personal gain." Google intentionally violated the enhanced penalty provision of 42 U.S.C. § 1320d-6 by acquiring the individually identifiable health information "with intent to sell transfer or use" it for "commercial advantage [or] personal gain";

d. To the extent that any particular at-issue communication or web property may be found to not be protected by HIPAA, Google's conduct is also prohibited by the FTC Act, as codified at 15 U.S.C. § 45, which provides that "unfair or deceptive acts or practices in or affecting commerce, are hereby declared illegal";

e. A knowing intrusion upon Plaintiffs' and Class Members' seclusion;

f. Trespass upon Plaintiffs' and Class Members' personal and private property via the placement of Google Cookies associated with the domains and patient portals for their Health Care Providers and covered entities on Plaintiffs' and Class Members' personal computing devices;

g. Violation of the California Unfair Competition Law, including by employing false, deceptive, or misleading advertising in its marketing of Google Ads and Analytics products to Health Care Providers;

h. Violation of the California Constitution's right to privacy, Section 1 of Article I of the California Constitution;

i. Violation of various state privacy statutes including, but not limited to, the CMIA; CCPA; CIPA, and Cal. Civ. Code § 1798.91;

j. Violation of various state computer privacy and property statutes, including but not limited to the California Comprehensive Computer Data Access and Fraud Act, Cal. Penal Code § 502; and,

k. Violation of Cal. Penal Code § 484 for statutory larceny, including by taking Plaintiffs' and Class Members' Health Information from Health Care Providers under the false pretense that it either was not Health Information or would not be transmitted.

223. Health Care Providers did not consent to the interceptions of Plaintiffs' and Class Members' communications containing Health Information.

a. Google failed to obtain consent to intercept personally identifiable information and its contracts with Health Care Providers suggested that Analytics and Ads Source Code could not be used to send personally identifiable information to Google even though the Source Code automatically intercepted identifiable information;

b. Google assured Health Care Providers using Google Signals that it had user consent to do so, but Google did not obtain user consent for collection of Health Information;

c. Google failed to obtain consent from Health Care Providers to connect a signed-out user's data to their account identifiers but did so anyway.

d. In the past year, several Health Care Providers have provided public notice of HIPAA breaches based on Google's interception of Health Information on Health Care Provider web-properties via the Google Source Code and each such

HCP has stated that its own actions that caused Google to intercept personally identifiable health information were not intentional.

224. Any purported consent provided by Health Care Providers had a purpose that was tortious, criminal, and in violation of state constitutional provisions, in that such conduct by the Health Care Provider constitutes:

a. A knowing intrusion into a private place, conversation, or matter that would be highly offensive to a reasonable person;

b. A violation of HIPAA, 42 U.S.C. § 1320d-6, which is a criminal offense punishable by fine or imprisonment and that includes increased penalties where "the offense is committed with intent to sell, transfer, or use individually identifiable health information for commercial advantage [or] personal gain";

c. Trespass;

d. Breach of fiduciary duty; and

e. Violation of various state privacy statutes including, but not limited to, the CMIA; CCPA; CIPA; and Cal. Civ. Code § 1798.91.

225. Google knows that its collection of Health Information from Health Care Providers is unlawful and tortious and intentionally obscured and downplayed the risk, known at all relevant times to Google and realized in practice as Google successfully deployed its third-party tracking technology to thousands of Health Care Provider web properties, that using Google Ads and Analytics products for their intended and widely advertised purposes, would result in Google's tortious acquisition of Class members' Health Information, violations of millions of United States patients' privacy, unlawful disclosure of health information under HIPAA, and the other harms and crimes alleged herein.

226. Google published an acknowledgement, incorporating the HHS Guidance, that Google Analytics products transmit Health Information when used for their intended purposes in or around March 2023 because its conduct was already subject to public scrutiny and attention from authorities. Google took no further action stop obtaining Health Information through Google

Analytics or otherwise, even though it has adequate information to identify all affected Health Care Provider web properties that transmit Health Information to it and has means of notifying them of the privacy violations in which they are, perhaps inadvertently, participating. Google also has means to stop the violations on its own by terminating Health Care Providers' use of Google Analytics on all webpages other than those which relate in no way to health or healthcare, providing a clear and direct notification that Google's third-party tracking technologies *cannot* be used without transmitting identifiable information, and updating its contracts, policies, Help pages, and communications with Google Analytics and Ads customers to clarify what Google actually does. Instead, Google continues to collect and use Health Information to serve its own purposes with full knowledge that it was collected in violation of HIPAA, which gives rise to criminal liability under 42 U.S.C. § 1320d-6, and various other state and common law torts and statutory causes of action listed herein, and appears to be waiting for all of the several thousand Health Care Providers involved in its conduct to realize that they have misunderstood how Google's services operate and face the civil and regulatory consequences on their own. By waiting for Health Care Providers to remove Google's third-party tracking technologies from their web properties, rather than taking action to stop the transmissions of Health Information on its own, Google has extended the length of time that many Class members' privacy rights will continue to be violated by a period of years, which has resulted in more Health Information flowing to Google's systems than Google would have obtained if it had taken timely action.

227. Google's violations of the ECPA were willful and intentional and caused Plaintiffs and Class Members the following damages:

a. The diminution in value of Plaintiffs' and Class Members' Health Information;

b. The loss of privacy due to Google making sensitive and confidential information, such as patient status, medical issues, and appointments, that Plaintiffs and Class Members intended to remain private no longer private; and

c. Google took something of value from Plaintiffs and Class Members and derived benefits therefrom without Plaintiffs' and Class Members' knowledge or informed consent and without Google sharing the benefit of such value.

228. For Google's violations set forth above, Plaintiffs and Class Members seek appropriate equitable and declaratory relief, including injunctive relief; actual damages and any profits made by Google as a result of its violations or the appropriate statutory measure of damages; punitive damages in an amount to be determined by a jury; and a reasonable attorney's fee and other litigation costs reasonably incurred pursuant to 18 U.S.C § 2520.

229. Unless enjoined, Google will continue to commit the violations of law alleged here. Plaintiffs and Class Members want to continue to communicate with their Health Care Providers through online platforms but have no practical way of knowing if their communications are being intercepted by Google, and thus continue to be at risk of harm from Google's conduct.

230. Pursuant to 18 U.S.C. § 2520, Plaintiffs and Class Members seek monetary damages for the greater of (i) the sum of the actual damages suffered by the Plaintiffs and any profits made by Google as a result of the violation or (ii) statutory damages of whichever is greater of $100 a day for each violation or $10,000.

COUNT TWO
VIOLATION OF THE CALIFORNIA INVASION OF PRIVACY ACT
(On Behalf of All Classes)

231. Plaintiffs hereby incorporate the factual allegations set forth above by reference.

232. CIPA is codified at Cal. Penal Code §§ 630-638. The Act begins with the following statement of purpose:

> The legislature hereby declares that advances in science and technology have led to the development of new devices and techniques for the purpose of eavesdropping upon private communications and that the invasion of privacy resulting from the continual and increasing use of such devices and techniques has created a serious threat to the free exercise of personal liberties and cannot be tolerated in a free and civilized society.

Cal. Penal Code § 630.

233. Cal. Penal Code § 631(a) provides, in pertinent part:

> Any person who, by means of any machine, instrument, or contrivance, or in any other manner …. willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads, or attempts to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable, or is being sent from, or received at any place within this state; or who uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained, or who aids, agrees with, employs, or conspires with any person or persons to lawfully do, or permit, or cause to be done any of the acts or things mentioned above in this section, is punishable by a fine not exceeding two thousand five hundred dollars.

234. There are no "vendor" or "agent" exceptions under Cal. Pen. Code § 631.

235. Cal. Penal Code § 632 provides, in pertinent part, that it is unlawful for any person "intentionally and without the consent of all parties to a confidential communication," to "use[] [a] recording device to … record the confidential communication."

236. As used in the statute, a "confidential communication" is:

> any communication carried on in circumstances as may reasonably indicate that any party to the communication desired it to be confined to the parties thereto[.]

237. Plaintiffs' and Class Members' Health Information, which was communicated with their Health Care Providers, constitutes confidential communications within the meaning of CIPA.

238. The Google Source Code constitutes a "device" within the meaning of CIPA § 632.

239. There are no "vendor" or "agent" exceptions under Cal. Pen. Code § 632.

240. Google is a "person" within the meaning of CIPA §§ 631 and 632.

241. Google is headquartered in California, designed, contrived, and effectuated its scheme to track, intercept, store, share and sell Plaintiffs' and Class Members' Health Information from California, and has adopted California substantive law to govern its relationship with users.

242. Google's learning or attempt to learn the contents of Plaintiffs' and Class Members' communications were intentional. As set forth above, Google targeted the healthcare industry to implement Google tracking technologies, knowing the use of the technologies on Health Care Provider web properties would transmit Health Information from patient visitors.

243. Google did not have the prior consent or authorization of all parties to obtain Plaintiffs' and Class Members' Health Information exchanged with their Health Care Providers, which includes the contents or record of their confidential communications.

244. Google's actions were designed to learn or attempt to learn the contents of Plaintiffs' and Class Members' electronic communications with their Health Care Providers.

245. Google's learning of or attempt to learn of the contents of Plaintiffs' and Class Members' electronic communications with Health Care Providers occurred while the communications were in transit or in the process of being sent or received.

246. Unless enjoined, Google will continue to commit the violations of law alleged here. Plaintiffs want to continue to communicate with their Health Care Providers and covered entities through online platforms but have no practical way of knowing if their communications are being intercepted by Google, and thus continue to be at risk of harm from Google's conduct.

247. Plaintiffs and Class Members seek all relief available under Cal. Penal Code § 637.2, including injunctive relief and statutory damages of $5,000 per violation or three times the actual amount of damages.

COUNT THREE
CALIFORNIA CONSTITUTIONAL INVASION OF PRIVACY
(On Behalf of All Classes)

248. Plaintiffs hereby incorporate the factual allegations set forth above by reference.

249. The California Constitution provides:

> *All people* are by nature free and independent and *have inalienable rights*. *Among these are* enjoying and defending life and liberty, acquiring, possessing, and protecting property, and *pursuing and obtaining* safety, happiness, and *privacy*.

Cal. Const. art. I, § 1 (emphasis added).

250. Plaintiffs and Class Members have both an interest in precluding the dissemination and misuse of their Health Information by Google, and in making intimate personal decisions and communicating with Health Care Providers without observation, intrusion or interference by Google.

251. Plaintiffs and Class Members had no knowledge of and did not consent or authorize Google to obtain their Health Information as described herein.

252. Plaintiffs and Class Members enjoyed objectively reasonable expectations of privacy surrounding their Health Information and communications devices used to exchange communications with their Health Care Providers, as evidenced by, among other things, federal, state and common laws that uphold the confidentiality of such information and that require lawful consent prior to disclosure.

253. Plaintiffs' and Class Members' claims are based on Google's unauthorized access to their Health Information as alleged herein, which includes, but is not limited to:

a. Plaintiffs' and Class Members' status as patients of a particular Health Care Provider;

b. Plaintiffs' and Class Members' communications while logged-in to "authenticated" pages on the Health Care Provider web properties, including the specific and detailed content of such communications, such as search terms, requests and responses for communications about appointments, doctors, treatments, conditions, health insurance, prescription drugs, and other Health Information;

c. Plaintiffs' and Class Members' communications with their Health Care Providers on "unauthenticated" portions of those properties, including the specific and detailed content of such communications, such as search terms and requests and responses for communications requesting information about appointments, doctors, treatments, conditions, health insurance, prescription drugs, and other Health Information; and

d. The ability to control and deny access to their communications devices while exchanging communications with their Health Care Providers on authenticated or unauthenticated pages.

254. In addition to acquiring Health Information without authorization, Google violated Plaintiffs' and Class Members' right to privacy in their communications devices by configuring

Google Source Code to deposit and disguise Google Cookies as "first-party" cookies belonging to Health Care Providers, when, in fact, they are third-party cookies belonging to Google.

255. Google's conduct was intentional and intruded on Plaintiffs' and Class Members' communications with their Health Care Providers, which constitute private conversations, matters, and data.

256. Google's conduct was highly offensive because, among other things:

a. Google conspired with Health Care Providers to violate a cardinal rule of the provider-patient relationship;

b. Google's conduct violated federal and state law designed to protect patient privacy, including but not limited to HIPAA and the CMIA;

c. Google's conduct violated the express promises it made to Google Account Holders; and

d. Google's conduct violated implied promises made to all users that it would not participate, enable, encourage, or profit from unlawful activity against Plaintiffs and Class Members.

257. Google's invasion of Plaintiffs' and Class Members' privacy resulted in the following damages:

a. Nominal damages for invasion of privacy;

b. General damages for invasion of their privacy rights in an amount to be determined by a jury without reference to specific pecuniary harm;

c. The diminution in value of Plaintiffs' and Class Members' Health Information;

d. Sensitive and confidential information including patient status and appointments that Plaintiffs and Class Members intended to remain private are no longer private;

e. Google eroded the essential confidential nature of the patient-provider relationship; and

f. Google took something of value from Plaintiffs and Class Members and derived benefits therefrom without Plaintiffs' and Class Members' knowledge or informed consent and without sharing the benefit of such value.

COUNT FOUR
INTRUSION UPON SECLUSION
(On Behalf of All Classes)

258. Plaintiffs hereby incorporate the factual allegations set forth above by reference.

259. By collecting and using the contents of Plaintiffs' and Class Members' communications with their Health Care Providers and covered entities without their knowledge, Google intentionally intruded into a realm in which Plaintiffs and Class Members have a reasonable expectation of privacy.

260. Plaintiffs and Class Members enjoyed objectively reasonable expectations of privacy in their communications with their Health Care Providers and covered entities relating to the respective patient portals, appointments, and Health Information and communications based on:

a. The Health Care Providers' or covered entities' status as their Health Care Providers or a covered entity and the reasonable expectations of privacy that attach to patient-provider relationships;

b. HIPAA;

c. The ECPA;

d. Google's promises that it will not use, or allow advertisers to use, Plaintiffs' and Class Members' Health Information for personalized advertising; and

e. California medical and computer privacy laws.

261. Furthermore, Plaintiffs and Class Members maintained a reasonable expectation of privacy when providing their Health Information to their Health Care Providers and covered entities and when communicating with their Health Care Providers and covered entities online.

262. Health Information is widely recognized by society as sensitive information that cannot be shared with third parties without the patients' consent.

263. For example, polling shows that "[n]inety-seven percent of Americans believe that doctors, hospitals, labs and health technology systems should not be allowed to share or sell their sensitive health information without consent."[108]

264. Google obtained unwanted access to Plaintiffs' and Class Members' Health Information, including, but not limited, to their patient status, the dates and times Plaintiffs and Class Members logged in to or out of patient portals, and the communications Plaintiffs and Class Members exchanged while logged in to patient portals.

265. In addition, Google intruded upon Plaintiffs' and Class Members' computing devices by gaining unauthorized access to those devices via web-bugs and "ghost cookies," i.e. cookies that are nominally set by the Health Care Provider web property to get around any efforts to prevent companies like Google from tracking consumers but that, in reality, belong to and are used by Google to surveil the Plaintiffs and Class Members.

266. Google's intrusion was accomplished by placing the _ga, _gid, __gcl_au, NID, IDE, DSID, and direct Google Account cookies on Plaintiffs' and Class Members' computing devices through the web-servers of Plaintiffs' and Class Members' Health Care Providers.

267. By disguising the _ga, _gid, and _gcl_au cookies as first-party cookies from Plaintiffs' Health Care Providers or covered entities, Google ensures that it can hack its way around attempts that Plaintiffs and Class Members might make to prevent Google's tracking through the use of cookie blockers.

268. In designing cookies as disguised first-party cookies, Google was aware that, like other websites that include sections where users sign in to an account, any Health Care Provider or covered entity website with a patient portal would require first-party cookies to be enabled for a patient to access the patient portal or other username / password protected 'secure' part of the Health Care Provider's website.

[108] *Poll: Huge majorities want control over health info*, HEALTHCARE FINANCE, (Nov. 10, 2010), https://www.healthcarefinancenews.com/news/poll-huge-majorities-want-control-over-health-info.

269. With first-party cookies being required for use of a patient portal and the Google cookies disguised as first-party cookies, Google was able to implant its tracking device on the computing devices of Plaintiffs and Class Members even where Plaintiffs or Class Members made attempts to stop third-party tracking through the use of cookie blockers.

270. Google's deployment of third-party cookies disguised as first-party cookies that are placed on Plaintiffs' and Class Members' computing devices is a highly offensive intrusion upon seclusion regardless of whether any information was further redirected from Plaintiffs' or Class Members' computing devices to Google.

271. Google's intrusion into Plaintiffs' and Class Members' privacy would be highly offensive to a reasonable person, namely because it occurred without Plaintiffs' and Class Members' consent or knowledge.

272. Google's intrusion caused Plaintiffs and Class Members the following damages:

a. Nominal damages;

b. The diminution in value of Plaintiffs' and Class Members' protected health information;

c. The loss of privacy due to Google making sensitive and confidential information such as patient status and appointments that Plaintiffs and Class Members intended to remain private no longer private; and

d. Google took something of value from Plaintiffs and Class Members and derived benefits therefrom without Plaintiffs' and Class Members' knowledge or informed consent and without Google sharing the benefit of such value.

273. Google's intrusion into Plaintiffs' and Class Members' seclusion was with oppression, fraud, or malice.

274. For Google's intrusion into their seclusion, Plaintiffs and Class Members seek actual damages, compensatory damages, restitution, disgorgement, general damages, nominal damages, unjust enrichment, punitive damages, and any other relief the Court deems just.

COUNT FIVE
BREACH OF CONTRACT
(On behalf of the Subclass of Google Account Holders)

275. Plaintiffs hereby incorporate the factual allegations set forth above by reference.

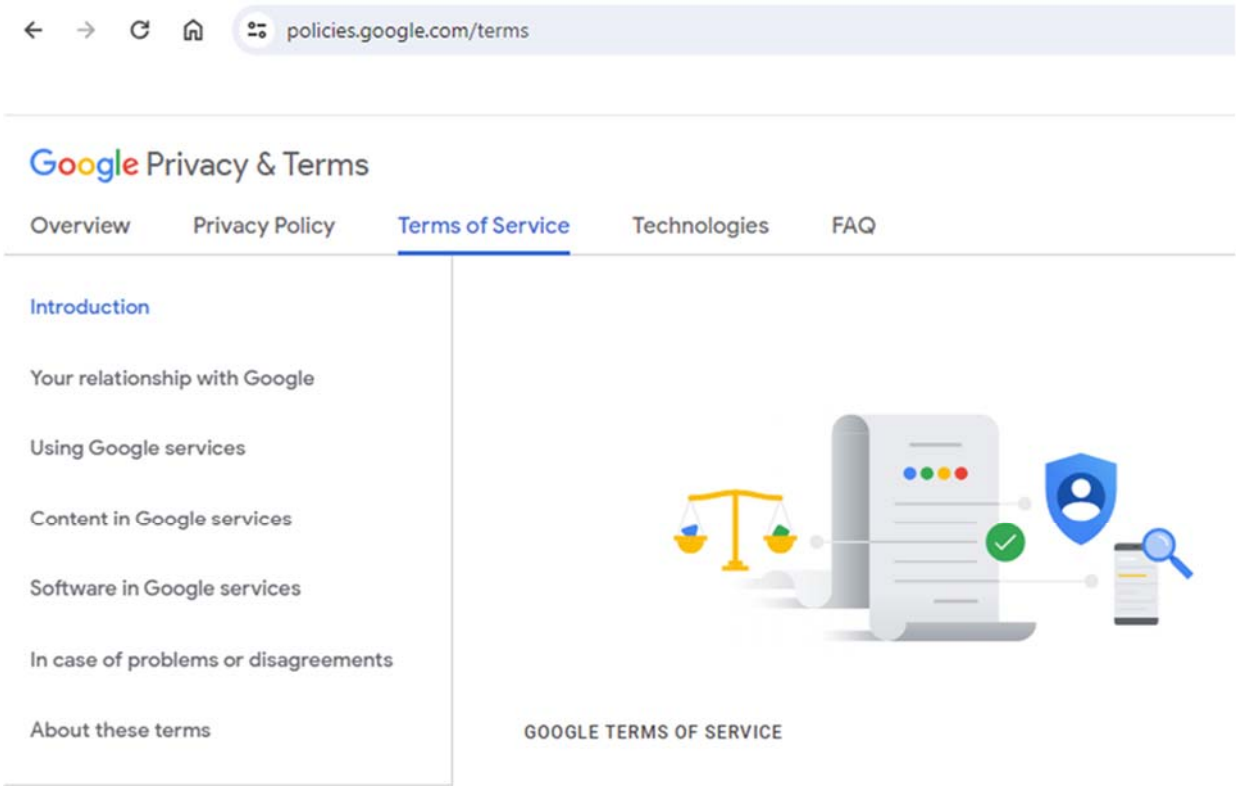
276. All Plaintiffs at all relevant times had Google Accounts and are members of the Google Account Holder Subclass.

277. The Google Terms of Service states that it "establish[es] what you can expect from [Google] as you use Google services, and what [Google] expect[s] from you." Google expressly identifies its Terms of Service document as a contract between Google and users, declaring that "by using our services, you're agreeing to these terms . . . ." and "you're contracting with: Google LLC." [109]

278. Plaintiffs briefly address questions of incorporation by reference. Exhibit 9 cited herein is a downloadable PDF version of Google's Terms of Service effective January 5, 2022. The PDF is not the form in which Google presents its contract to users. Google makes the PDF available on its website but does not require that the PDF be downloaded or viewed to be binding. Instead, Google presents its Terms of Service to users as one of five webpages at the URL https://policies.google.com/terms. This URL is accessible via a "Terms" hyperlink at the bottom of numerous Google webpages, including the webpage to create a Google Account, to sign in, and to manage an account after logging in. These five webpages, titled: "Overview," "Privacy Policy,"

[109] Ex. 9, *Terms of Service*, at 1-2 (stating "these Terms of Service help define Google's relationship with you as you interact with our services" (emphasis added) and that "by using our services, you're agreeing to these terms").

"Terms of Service," "Technologies," and "FAQ," are nested within a broader "Google Privacy & Terms" website, as follows:



279. The tab titled "Overview" links to the "Privacy & Terms" Overview main page, which displays a menu bar in the upper left-hand corner with the same five menu options. The "Privacy Policy" menu option links to Google's Privacy Policy webpage at the URL https://policies.google.com/privacy, containing additional hyperlinked menu options. [110] The "Terms of Service" menu option links to the Terms of Service webpage at the URL https://policies.google.com/terms, containing additional hyperlinked menu options. The "Technologies" menu option links to Google's Policies Site/Technologies webpage at the URL https://policies.google.com/technologies, containing one paragraph of text and under the heading

[110] Google has changed the text in its Privacy Policy twice since this action was filed in May 2023, on July 1, 2023 and October 4, 2023. Plaintiffs refer herein to the version of Google's Privacy Policy effective December 2022, which was in effect at the time this action was filed. A downloadable PDF copy of the December 2022 version of Google's Privacy Policy is attached as Exhibit 14. As with the Terms of Service, Google imposes no requirement that users review the downloadable PDF version of its Privacy Policy.

"Technologies," and additional hyperlinked menu options, including one for "Advertising." The "FAQ" menu option links to Google's Frequently asked Questions webpage at the URL https://policies.google.com/faq, containing additional hyperlinks.

280. Google's Terms of Service do not purport to exclude additional Google policies and terms from the scope of each user's contractual agreement with Google. On the contrary, they state that "these Terms of Service *help* define Google's relationship with you," which, like Google's presentation of the Terms of Service as one of numerous policy documents, indicates that the Terms of Service do not exclusively define the contractual relationship.[111] The Google Terms of Service webpage, like the Privacy & Terms Overview website of which it is a part, refers to and incorporates a large number of other Google-authored webpages.

281. The Google Terms of Service also expressly incorporate the Google Privacy Policy webpage, and the Technologies/Policies Site webpage, declaring, "You also agree that our Privacy Policy applies to your use of our services. Additionally, we provide resources like the Copyright Help Center, Safety Center, and descriptions of our technologies from our policies site to answer common questions and to set expectations about using our services," where the underlined "Privacy Policy" text hyperlinks to the same Privacy Policy webpage, and the underlined "policies site" text hyperlinks to the same Technologies/Policies Site webpage, that are accessible from the hyperlinks surrounding the nested Terms of Service and the Privacy & Terms Overview webpage main menu.[112]

282. The contents of these policies are drafted exclusively by Google. Google presents these terms online, in an interactive format, with the full scope of information viewable only via a complex web of hyperlinks to which all users of Google products and services must agree without alteration, in order for Google to permit their use of Google products and services. Together, they form an express contract.

283. Plaintiffs and Class Members did all they were required to do under the contract.

[111] Ex. 9, *Terms of Service*, at 1 (emphasis added).

[112] Ex. 9, *Terms of Service*, at 4, and hyperlinks therein.

284. Within the interconnected web of policies that form Google's contract, Google makes at least two promises that it has violated through its conduct alleged herein:

285. Promise 1: Google promises that Google does not collect Health Information that individuals do not choose to provide to Google. Under the sub-heading "Categories of information we collect," the Google Privacy Policy identifies "health information" as a distinct category of information, and explains that Google's collection of this information is limited to only when a person "choose[s] to provide it": "Health information *if you choose to provide it*, such as your medical history, vital signs and health metrics (like blood glucose levels), and other similar information related to your physical or mental health, in the course of using Google services that offer health-related features, such as the Google Health Studies app."[113]

286. Google materially breached Promise 1 by collecting the Health Information of Plaintiffs and Class Members through the automatic operation of Google Source Code when Plaintiffs and Class Members did not choose to provide it; by failing to respect the privacy rights of Plaintiffs and Class Members with its own acquisition and use of their Health Information, and by encouraging Health Care Providers to use Google Source Code in violation of those rights, rather than terminating their use of Google services upon learning of the violations.

287. Promise 2: Google promises not to use Health Information for personalized advertising. Under the heading "Why Google Collects Data," in Google's Privacy Policy, Google declares that "You can control what information we use to show you ads by visiting your ad settings in My Ad Center. . . . " It continues that Google does not show "personalized ads based on sensitive categories," such as . . . health, where the underlined text expands to declare: "When showing you personalized ads, . . . [w]e don't use topics or show personalized ads based on sensitive categories like race, religion, sexual orientation, or health. And we require the same from advertisers that use our services."[114] The hyperlinked text "require the same from advertisers"

[113] Ex. 14, *Privacy Policy*, at 17-18 (emphasis added).

[114] Ex. 14, *Privacy Policy*, at 5-6, 30 (underline/hyperlink original).

links to Google's "Advertising Policies Help" webpage, at the URL https://support.google.com/adspolicy/answer/143465.

288. Plaintiff again briefly addresses incorporation by reference. Similar to Google's nested presentation of Google's Terms of Service as one of five menu options, the Advertising Policies Help webpage contains four tabs along the top, each of which, if clicked, reveals a different portion of the webpage. The "List of ad policies" tab is selected by default at the hyperlink from Google's Privacy Policy, and the "Personalized advertising" policy,[115] one of several policy documents available under that menu option, is displayed. This page contains a description of advertising policies, numerous additional hyperlinks, and a list of other hyperlinked policies on its right-hand side.

289. Google repeats and expands upon its promises in the Personalized advertising policy, where Google promises that it prohibits advertising based on: "Restricted drug terms," such as "prescription medications and information about prescription medications . . . .;" and "personal health content," such as "physical or mental health conditions, including diseases, sexual health, and chronic health conditions"; "[p]roducts, services, or procedures to treat or manage chronic health conditions…"; "any health issues associated with intimate body parts or functions…"; "invasive medical procedures"; and, "[d]isabilities, even when content is oriented toward the user's primary caretaker," and again confirms that "**We don't allow targeting users** based on legally restricted content."[116]

290. A reasonable person reading the contract would understand that Google does not use Health Information for any advertising purpose, to target users in any way, or to personalize or tailor any product or service. A reasonable person reading the contract would understand that to the extent Google receives Health Information, Google maintains that information separately from the data that it uses for other business purposes, and neither accesses nor allows access to the information to be accessed, except to fulfill the specific purposes for which it was obtained.

[115] Ex. 15, *Personalized Advertising*.

[116] *Id.* at 4, 5, 8.

291. Google materially breached Promise 2 by using Health Information in advertising products and services that are personalized, including through using "past web traffic Google noticed" to inform its Placements products and using Health Information to develop, maintain, and improve its artificial intelligence systems for advertising. Google materially breached Promise 2 by targeting users based upon Health Information with personalized "content" including recommendations and otherwise personalizing Google's products and services based Health Information. Google materially breached Promise 2 by using Health Information for other business purposes, including without limitation in connection with its efforts to develop new products, services, and businesses in the healthcare industry.

292. Google's breach caused Plaintiffs and Class Members the following damages:

a. Nominal damages for breach of contract;

b. General damages for invasion of their privacy rights in an amount to be determined by a jury without reference to specific pecuniary harm;

c. Damages resulting from their loss of control over sensitive and confidential information including patient status and appointments that Plaintiffs and Class Members intended to remain private which are no longer private;

d. Google eroded the essential confidential nature of the patient-provider relationship;

e. Google took something of value from Plaintiffs and Class Members and derived benefits therefrom without Plaintiffs' and Class Members' knowledge or informed consent and without sharing the benefit of such value; and,

f. Benefit of the bargain damages in that Google's contract stated that payment for the service would consist of a more limited set of collection of personal information than that which Google actually charged.

COUNT SIX
GOOD FAITH AND FAIR DEALING
(On behalf of the Subclass of Google Account Holders)

293. Plaintiffs hereby incorporate the factual allegations set forth above by reference.

294. A valid contract exists between Plaintiffs and Google.

295. The contract specifies that California law governs the parties' relationship.

296. Google prevented Plaintiffs and Class Members from receiving the full benefit of the contract by intercepting their Health Information.

297. By doing so, Google abused its power to define terms of the contract, including but not limited to:

a. Google's effort to limit the meaning of "Health Information" to something that is not consistent with what any reasonable person would understand and directly contrary to federal and state laws, as well as patients' reasonable expectations of privacy;

b. Google's effort to change the meaning of the term "identifiable" in its statements to publishers and advertisers in a way that is directly contrary to (i) the plain English meaning of the term; (ii) federal and state law; and (iii) the definitions of "personal information" under Google's Privacy Policy and California law; and

c. Google's effort to interpret "personalized advertising" to exclude remarketing, conversion tracking, targeting contextual advertising, and other advertising uses based on Health Information and communications of Plaintiffs and Class Members their Health Care Provider web properties.

298. By doing so, Google did not act fairly and in good faith.

299. Google's breach caused Plaintiffs and Class Members the following damages:

a. Nominal damages for breach of contract;

b. General damages for invasion of their privacy rights in an amount to be determined by a jury without reference to specific pecuniary harm;

c. Sensitive and confidential information including patient status and appointments that Plaintiffs and Class Members intended to remain private are no longer private;

d. Google eroded the essential confidential nature of the patient-provider relationship;

e. Google took something of value from Plaintiffs and Class Members and derived benefits therefrom without Plaintiffs' and Class Members' knowledge or informed consent and without sharing the benefit of such value; and

f. Benefit of the bargain damages in that Google's contract stated that payment for the service would consist of a more limited set of collection of personal information than that which Google actually charged.

COUNT SEVEN
UNJUST ENRICHMENT UNDER CALIFORNIA COMMON LAW
(On Behalf of All Classes)

300. Plaintiffs hereby incorporate the factual allegations set forth above by reference.

301. California common law on unjust enrichment is applicable for all members of the U.S. Health User Class.

302. Google has wrongfully and unlawfully trafficked in the named Plaintiffs' and the Class Members' Health Information and other personal data without their consent for substantial profits.

303. Plaintiffs' and Class Members' Health Information and data have conferred an economic benefit on Google.

304. Google has been unjustly enriched at the expense of Plaintiffs and Class Members, and the company has unjustly retained the benefits of its unlawful and wrongful conduct.

305. The remedies available to Plaintiffs' and Class Members are inadequate to compensate them for the injuries they have suffered as a result of Google's conduct. Thus, it would be inequitable and unjust for Google to be permitted to retain any of the unlawful proceeds resulting from its unlawful and wrongful conduct.

306. A portion—but not all—of the unjust enrichment Google obtained was through the Plaintiffs' and Class Members' use of Health Care Provider web properties, which constitutes an invasion of privacy. Moreover, the access Plaintiffs and Class Members received to those web

properties does not defeat their unjust enrichment claim because Plaintiffs were not aware of Google's conduct while communicating with their Health Care Providers on the Health Care Providers' web properties and did not and could not consent to that conduct. Had Plaintiffs known of Google's conduct, Plaintiffs would not have visited those websites or, if such visits were unavoidable, would have taken additional precautions to avoid being tracked and profiled by Google. Google's conduct with respect to tracking Plaintiffs' conduct on any web properties cannot be viewed in isolation—the aggregation, compilation, analysis, and use of that extensive information about Plaintiffs' habits—and personal and private medical communications—violates Plaintiffs' California Constitutional and common law rights. Moreover, the fruits of Google's illegal wiretapping of Plaintiffs' communications with Health Care Provider web properties, in violation of criminal statutes, also contributed to Google's enrichment. Google's enrichment through violation of criminal wiretapping statutes is inherently unjust.

307. Plaintiffs did not provide authorization for the use of their information, nor did Google provide them with control over its use.

308. Plaintiffs' aggregate Health Information carries financial value. Google was unjustly enriched by aggregating Plaintiffs' personal and sensitive Health Information and monetizing that data to obtain financial gain.

309. The portion of Google's revenue attributable to Google's wrongful conduct described herein is susceptible of measurement and can be determined through discovery.

310. It would be unjust and inequitable to allow Google to profit from its violation of the Plaintiffs' and Class Members' Constitutional, common law, and statutory rights as described herein. Google's conduct in collecting and using Plaintiffs' and Class Members' private Health Information is conduct that was specifically singled out for disapprobation by the voters of California in amending the California Constitution. Google's conduct is highly offensive to a reasonable person, and as such, regardless of whether Plaintiffs and Class Members received anything of value from the web properties they visited, Google's profiting from its collection and use of their data violates California public policy and goes well beyond acceptable social norms.

311. Google was aware of the benefit conferred by Plaintiffs and Class Members. Google acted in conscious disregard of the rights of Plaintiffs and Class Members and should be required to disgorge all profit obtained therefrom to deter Google and others from committing the same unlawful actions again.

IX. PRAYER FOR RELIEF

WHEREFORE, Plaintiffs respectfully request that this Court:

A. Certify the proposed Classes, designating Plaintiffs as the named representatives of the Class and Subclass, and designating the undersigned as Class Counsel;

B. Permanently restrain Defendant, and its officers, agents, servants, employees and attorneys, from using Google Source Code to track, obtain and use Plaintiffs' and Class Members' Health Information;

C. Award compensatory damages, including statutory damages where available, to Plaintiffs and the Class against Google for all damages sustained as a result of Google's wrongdoing, in an amount to be proven at trial, including interest thereon;

D. Award punitive damages on the causes of action that allow for them and in an amount that will deter Google and others from like conduct;

E. Enter judgment in favor of Plaintiffs and the members of the Class against Google awarding unjust enrichment and/or restitution of Google's ill-gotten gains, revenues, earnings, or profits that it derived, in whole or in part, from its unlawful collection and use of Class Members' personal data, in an amount according to proof at trial;

F. Award attorneys' fees and costs, as allowed by law including, but not limited to, California Code of Civil Procedure section 1021.5;

G. Award pre-judgment and post-judgment interest, as provided by law; and

H. For such other, further, and different relief as the Court deems proper under the circumstances.

X. DEMAND FOR JURY TRIAL

Pursuant to F.R.C.P. Rule 38, Plaintiffs, on behalf of themselves and the Classes, demand a trial by jury of any and all issues in this action so triable of right.

Dated: August 12, 2024

SIMMONS HANLY CONROY LLC

/s/ Jay Barnes
Jason 'Jay' Barnes

Jason 'Jay' Barnes (admitted *pro hac vice*)
jaybarnes@simmonsfirm.com
Eric Johnson (admitted *pro hac vice*)
ejohnson@simmonsfirm.com
An Truong (admitted *pro hac vice*)
atruong@simmonsfirm.com
112 Madison Avenue, 7th Floor
New York, NY 10016
Tel.: 212-784-6400
Fax: 212-213-5949

Dated: August 12, 2024

LOWEY DANNENBERG, P.C.

/s/ Christian Levis
Christian Levis

Christian Levis (admitted *pro hac vice*)
clevis@lowey.com
Amanda Fiorilla (admitted *pro hac vice*)
afiorilla@lowey.com
44 South Broadway, Suite 1100
White Plains, NY 10601
Tel: (914) 997-0500
Fax: (914) 997-0035

KIESEL LAW LLP

Jeffrey A. Koncius, State Bar No. 189803
koncius@kiesel.law
Nicole Ramirez, State Bar No. 279017
ramirez@kiesel.law
Kaitlyn Fry, State Bar No. 350768
fry@kiesel.law
8648 Wilshire Boulevard
Beverly Hills, CA 90211-2910
Tel: 310-854-4444
Fax: 310-854-0812

LIEFF CABRASER HEIMANN & BERNSTEIN, LLP

Michael W. Sobol (State Bar No. 194857)
msobol@lchb.com
Melissa Gardner (State Bar No. 289096)
mgardner@lchb.com
Jallé H. Dafa (State Bar No. 290637)
jdafa@lchb.com
275 Battery Street, 29th Floor
San Francisco, CA 94111-3339
Tel: 415 956-1000
Fax: 415-956-1008

Douglas Cuthbertson (admitted *pro hac vice*)
dcuthbertson@lchb.com
250 Hudson Street, 8th Floor
New York, NY 10013
Tel: 212 355-9500
Fax: 212-355-9592

SCOTT+SCOTT ATTORNEYS AT LAW LLP

Hal D. Cunningham (Bar No. 243048)
hcunningham@scott-scott.com
Sean Russell (Bar No. 308962)
srussell@scott-scott.com
600 W. Broadway, Suite 3300
San Diego, CA 92101
Tel: (619) 233-4565
Fax: (619) 233-0508

Joseph P. Guglielmo (admitted *pro hac vice*)
jguglielmo@scott-scott.com
Ethan Binder (admitted *pro hac vice*)
ebinder@scott-scott.com
230 Park Ave., 17th Floor
New York, NY 10169
Telephone: (212) 223-6444
Facsimile: (212) 223-6334

Attorneys for Plaintiffs and the Proposed Class

ATTESTATION

Pursuant to Civil Local Rule 5-1(h)(3), I hereby attest that all signatories listed, and on whose behalf the filing is submitted, concur in the filing's content and have authorized the filing.

Dated: August 12, 2024

/s/ Melissa Gardner
Melissa Gardner

APPENDIX A: INDEX OF EXHIBITS

No.	Name	URL
Exhibit 1	Sample Findings of Investigation of Plaintiff Health Care Provider web properties: *Screenshots of Fiddler Records*	N/A, but see https://learn.microsoft.com/en-us/windows/win32/win7appqual/fiddler-web-debugger-toolfor a discussion of Fiddler
Exhibit 2	Sample Findings of investigation of Plaintiff Health Care Provider web properties: *Excerpt of HTTP Header Transmissions*	N/A
Exhibit 3	*Important notice about a privacy matter*, KAISER PERMANENTE (May 6, 2024)	https://healthy.kaiserpermanente.org/washington/alerts/p3/privacy-matter
Exhibit 4	April 22, 2022 email correspondence with Gordon-Nguyen, Marissa (HHS/OCR), *Am. Hospital Ass'n v. Becerra*, No. 23-cv-01110-P (N.D. Tex.), Dkt. 49-8.	N/A
Exhibit 5	Ari B. Friedman, et al., *Prevalence of Third-Party Tracking on Abortion Clinic Web Pages*, JAMA (Sept. 8, 2022), at 274-275	https://jamanetwork.com/journals/jamainternalmedicine/fullarticle/2796236
Exhibit 6	*Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates*, U.S. DEP'T OF HEALTH AND HUM. SERV. (Dec. 1, 2022)	https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html
Exhibit 7	*HHS Bulletin on Tracking Technologies: Index to the Administrative Record* (filed in *Am. Hospital Ass'n v. Becerra*, No. 4:23-cv-01110-P (N.D. Tex.), Dkt. 49-2)	
Exhibit 8	*Measurement Protocol Parameter Reference*, GOOGLE FOR DEVELOPERS/ANALYTICS	https://developers.google.com/analytics/devguides/collection/protocol/v1/parameters
Exhibit 9	*Terms of Service*, GOOGLE PRIVACY & TERMS (downloadable PDF) (Jan. 5, 2022)	https://policies.google.com/terms/archive/20220105
Exhibit 10	*2017 Strategy Paper: Measurement*, GOOGLE (filed Aug. 6, 2024 in *United States v. Google LLC*, No. 1:23-cv-00108-LMB-JFA (E.D. Va. 2023), Dkt. 1132-2)	N/A
Exhibit 11	*2017 Charter: Google Analytics*, Google, (filed Aug. 6, 2024 in *United States v. Google LLC*, No. 1:23-cv-00108-LMB-JFA (E.D. Va. 2023), Dkt. 1132-2)	N/A
Exhibit 12	Lee Fifield, *Advocate Aurora Health Data Breach Affects 3 Million Patients*, AAPC (October 27, 2022)	https://www.aapc.com/blog/86572-advocate-aurora-health-data-breach-affects-3-million-patients
Exhibit 13	*Notice of data privacy incident from Allina Health*, ALLINA HEALTH (April 28, 2023)	https://www.allinahealth.org/about-us/news-releases/2023/notice-of-data-privacy-incident-from-allina-healthE
Exhibit 14	*Privacy Policy*, GOOGLE PRIVACY & TERMS (Dec. 15, 2022) (downloadable PDF)	https://policies.google.com/privacy/archive/20221215
Exhibit 15	*Personalized Advertising*, GOOGLE ADVERTISING POLICIES HELP (print-friendly reproduction)	https://support.google.com/adspolicy/answer/143465